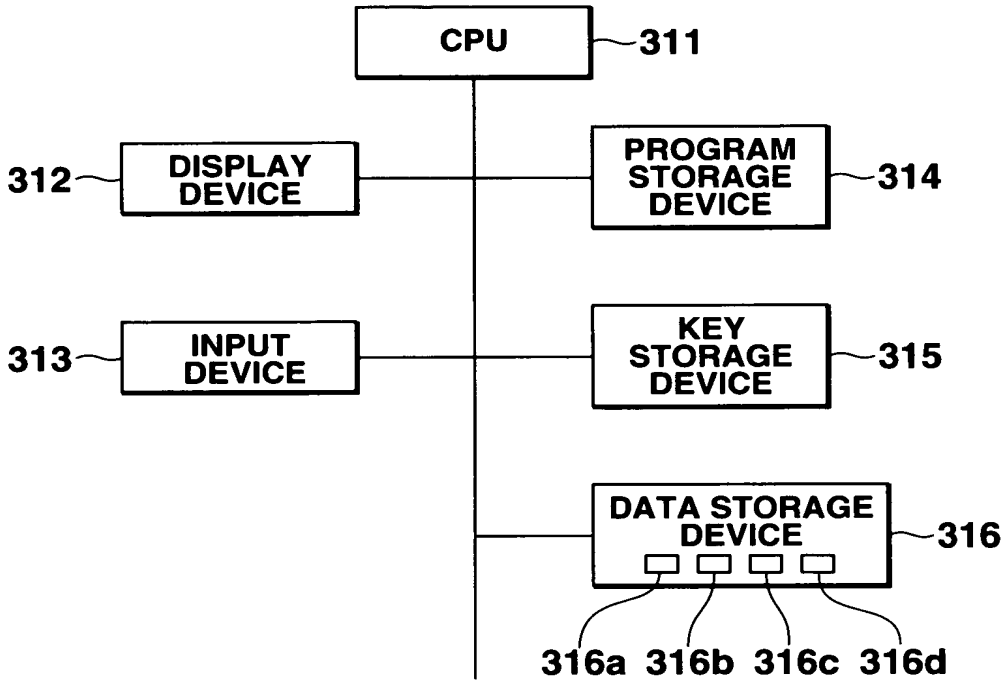
CPU
311
312
DISPLAY DEVICE
PROGRAM STORAGE DEVICE
314
313
INPUT DEVICE
KEY STORAGE DEVICE
315
DATA STORAGE DEVICE
316
316a
316b
316c
316d

FIG.1

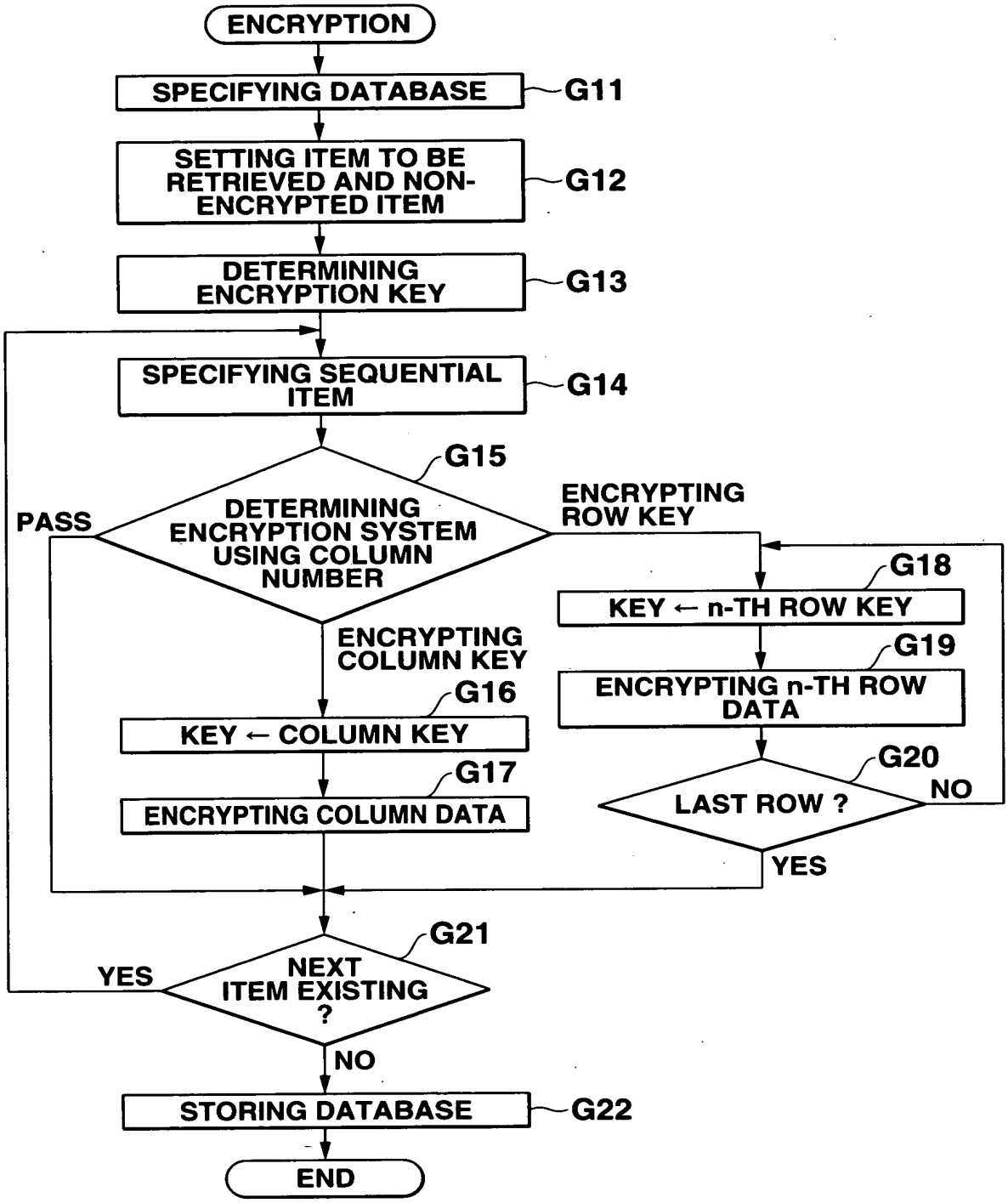
ENCRYPTION
SPECIFYING DATABASE
G11
SETTING ITEM TO BE RETRIEVED AND NON-ENCRYPTED ITEM
G12
DETERMINING ENCRYPTION KEY
G13
SPECIFYING SEQUENTIAL ITEM
G14
G15
DETERMINING ENCRYPTION SYSTEM USING COLUMN NUMBER
PASS
ENCRYPTING ROW KEY
ENCRYPTING COLUMN KEY
G16
KEY ← COLUMN KEY
G17
ENCRYPTING COLUMN DATA
G18
KEY ← n-TH ROW KEY
G19
ENCRYPTING n-TH ROW DATA
G20
LAST ROW ?
NO
YES
G21
NEXT ITEM EXISTING ?
YES
NO
STORING DATABASE
G22
END

FIG.2

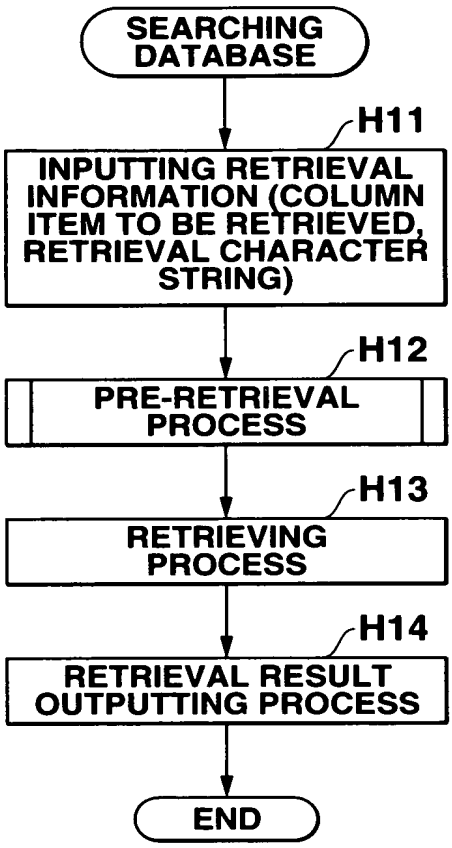
SEARCHING DATABASE
H11
INPUTTING RETRIEVAL INFORMATION (COLUMN ITEM TO BE RETRIEVED, RETRIEVAL CHARACTER STRING)
H12
PRE-RETRIEVAL PROCESS
H13
RETRIEVING PROCESS
H14
RETRIEVAL RESULT OUTPUTTING PROCESS
END

FIG.3A

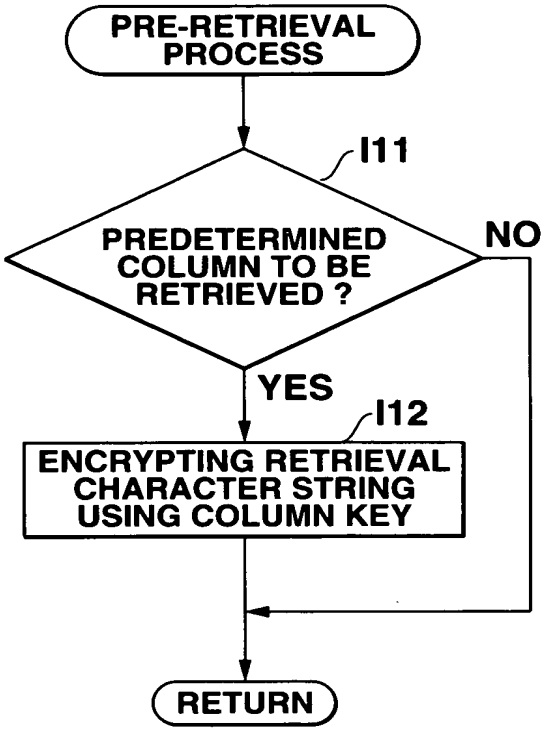
PRE-RETRIEVAL PROCESS
I11
PREDETERMINED COLUMN TO BE RETRIEVED ?
NO
YES
I12
ENCRYPTING RETRIEVAL CHARACTER STRING USING COLUMN KEY
RETURN

FIG.3B

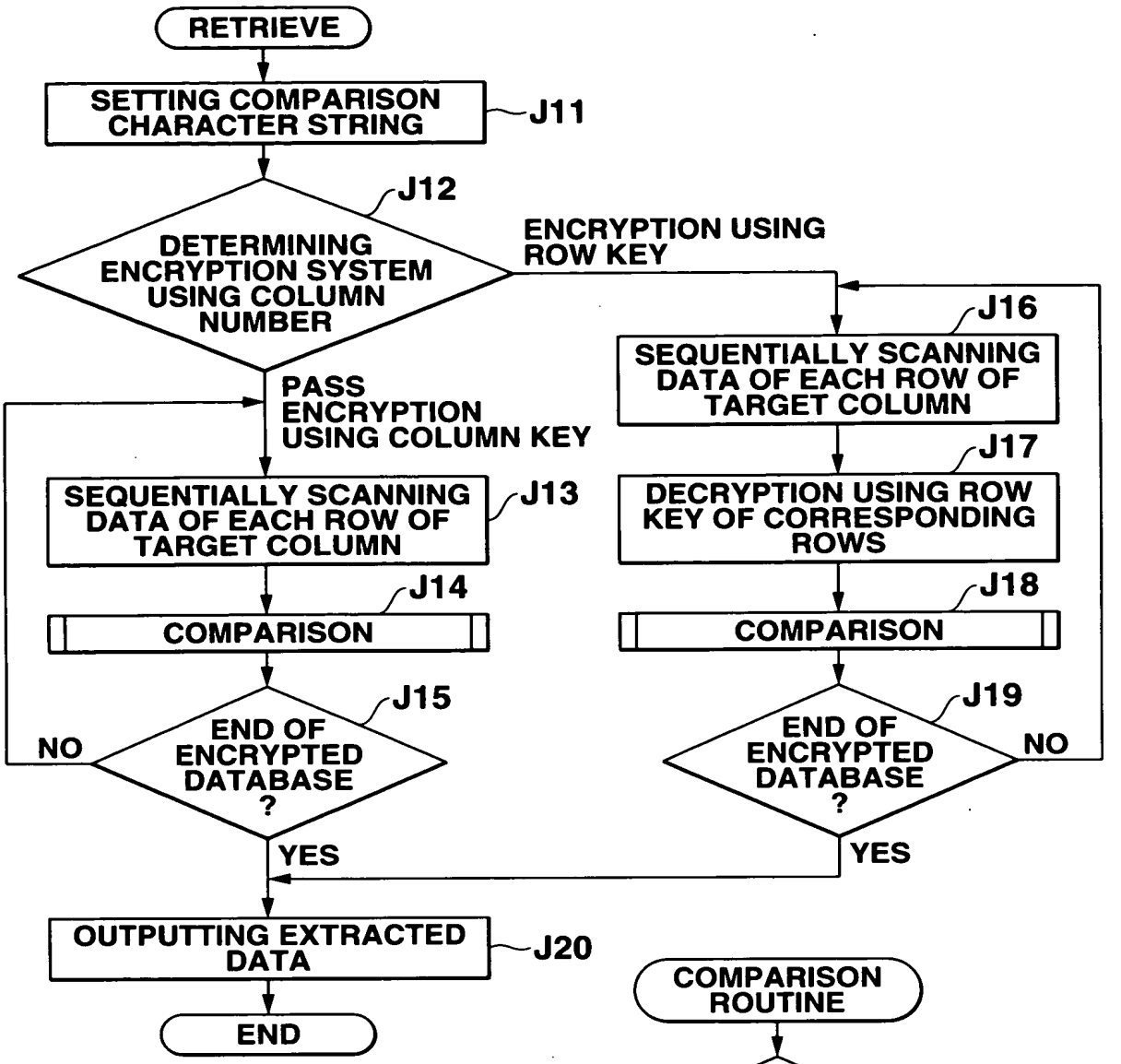
RETRIEVE
SETTING COMPARISON CHARACTER STRING
J11
J12
DETERMINING ENCRYPTION SYSTEM USING COLUMN NUMBER
ENCRYPTION USING ROW KEY
PASS ENCRYPTION USING COLUMN KEY
J16
SEQUENTIALLY SCANNING DATA OF EACH ROW OF TARGET COLUMN
J17
DECRYPTION USING ROW KEY OF CORRESPONDING ROWS
SEQUENTIALLY SCANNING DATA OF EACH ROW OF TARGET COLUMN
J13
J14
COMPARISON
J18
COMPARISON
J15
END OF ENCRYPTED DATABASE ?
NO
J19
END OF ENCRYPTED DATABASE ?
NO
YES
YES
OUTPUTTING EXTRACTED DATA
J20
END

FIG.4A

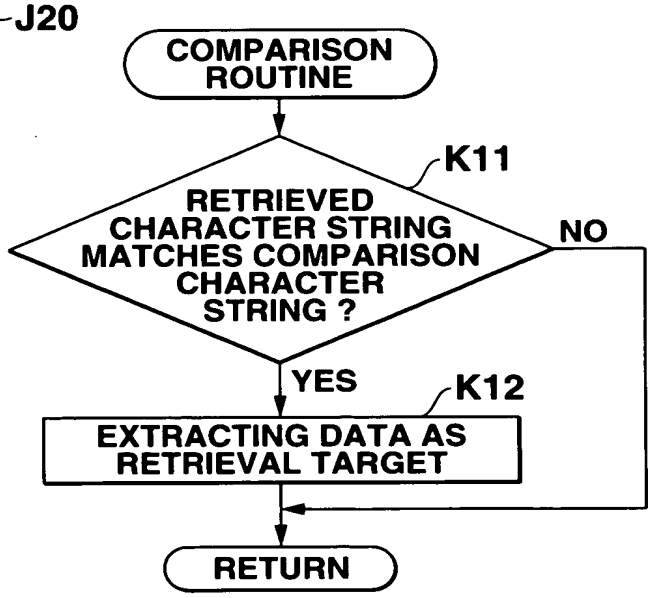
COMPARISON ROUTINE
K11
RETRIEVED CHARACTER STRING MATCHES COMPARISON CHARACTER STRING ?
NO
YES
K12
EXTRACTING DATA AS RETRIEVAL TARGET
RETURN

FIG.4B

(a)

number	name	state	weight	height	age	phone
1	Jhon	New York	63	130	22	407-228-6611
2	Chris	Florida	72	190	21	123-456-7890
3	Michael	Minnesota	65	163	27	101-202-3030
4	David	Iowa	63	145	34	523-761-0045
5	Mark	New York	65	152	30	832-962-9001
6	Daniel	Iowa	68	170	25	231-981-9454
7	George	Idaho	69	180	31	561-545-4389
8	Henry	Florida	71	165	22	239-203-9800
9	Joe	New Jersey	66	163	27	239-129-9898

ENCRYPTION ↓ COLUMN KEY ROW KEY

(b)

number	name	state	weight	height	age	phone
1	wJls	noevjolc	qw	ywe	jh	igdltytfhDSk
2	ddGGa	h*/fDD	lr	Erw	hg	LKtYtDSkoKow
3	1jkjl+P	gah{6xpVd	RK	Tyi	tY	hkliiydageQk
4	3eK@s	kHHS	kd	DHH	Kl	d+fDlKnBerJf
5	erlN	noevjolc	jD	iOO	Gv	wsdERfvW2Sdf
6	F>sSlu	kHHS	8u	lki	ij	1xcVlmFmkjpo
7	(:ld?k	lJHFD	HH	lpa	LK	kjwDkJGvfDoa
8	rhJKd	h*/fDD	ew	Aii	jh	e419h-ka+qwH
9	ifd	ASoChijlO-	Df	lky	tY	qLFUiCVkj@kl

DECRYPTION ↓ COLUMN KEY ROW KEY

(c)

number	name	state	weight	height	age	phone
1	Jhon	New York	63	130	22	407-228-6611
2	Chris	Florida	72	190	21	123-456-7890
3	Michael	Minnesota	65	163	27	101-202-3030
4	David	Iowa	63	145	34	523-761-0045
5	Mark	New York	65	152	30	832-962-9001
6	Daniel	Iowa	68	170	25	231-981-9454
7	George	Idaho	69	180	31	561-545-4389
8	Henry	Florida	71	165	22	239-203-9800
9	Joe	New Jersey	66	163	27	239-129-9898

FIG.5

COLUMN KEY

number	name	state	weight	height	age	phone
NONE	"apple"	"orange"	ROW KEY	ROW KEY	"lemon"	ROW KEY

ROW KEY

number	
1	"tiger"
2	"dog"
3	"cat"
4	"mouse"
5	"elephant"
6	"cow"
7	"pig"
8	"rabbit"
9	"lion"

FIG.6

(a)

number	name	state	weight	height	age	phone
1	Jhon	New York	63	130	22	407-228-6611
2	Chris	Florida	72	190	21	123-456-7890
3	Michael	Minnesota	65	163	27	101-202-3030
4	David	Iowa	63	145	34	523-761-0045
5	Mark	New York	65	152	30	832-962-9001
6	Daniel	Iowa	68	170	25	231-981-9454
7	George	Idaho	69	180	31	561-545-4389
8	Henry	Florida	71	165	22	239-203-9800
9	Joe	New Jersey	66	163	27	239-129-9898

ENCRYPTION | COMPOSITE KEY

(b)

number	name	state	weight	height	age	phone
1	wJls	noevjolc	xo	qwe	jh	dfghaJ;lkqlu
2	ddGGa	h*/fDD	wi	klA	hg	qwTylBnDFiKj
3	1jkjl+P	gah{6xpVd	hi	lKJ	tY	DafgiqlkimD-
4	3eK@s	kHHS	s?	SGA	Kl	hi*khaTygfXd
5	erlN	noevjolc	d-	ASD	Gv	8uyDBmAkolka
6	f>sSlu	kHHS	l*	qoK	ij	jhtvbnMKJASW
7	(:ld?k	lJHFD	df	sLL	LK	lQwSRyuiokjq
8	rhJKd	h*/fDD	Ws	tyH	of	Dfha*kaqil
9	ifd	ASoChijlO-	qo	H2a	Ga	lkjHYAGoiuq

DECRYPTION | COMPOSITE KEY

(c)

number	name	state	weight	height	age	phone
1	Jhon	New York	63	130	22	407-228-6611
2	Chris	Florida	72	190	21	123-456-7890
3	Michael	Minnesota	65	163	27	101-202-3030
4	David	Iowa	63	145	34	523-761-0045
5	Mark	New York	65	152	30	832-962-9001
6	Daniel	Iowa	68	170	25	231-981-9454
7	George	Idaho	69	180	31	561-545-4389
8	Henry	Florida	71	165	22	239-203-9800
9	Joe	New Jersey	66	163	27	239-129-9898

FIG.7

COMPOSITE KEY

number	name	state	weight	height	age	phone
NONE	"apple"	"orange"	"bananatiger"	"lycheetiger"	"lemon"	"apricottiger"
NONE	"apple"	"orange"	"bananadog"	"lycheedog"	"lemon"	"apricotdog"
NONE	"apple"	"orange"	"bananacat"	"lycheecat"	"lemon"	"apricotcat"
NONE	"apple"	"orange"	"bananamouse"	"lycheemouse"	"lemon"	"apricotmouse"
NONE	"apple"	"orange"	"bananaelephant"	"lycheeelephant"	"lemon"	"apricotelephant"
NONE	"apple"	"orange"	"bananacow"	"lycheecow"	"lemon"	"apricotcow"
NONE	"apple"	"orange"	"bananapig"	"lycheepig"	"lemon"	"apricotpig"
NONE	"apple"	"orange"	"bananarabbit"	"lycheerabbit"	"lemon"	"apricotrabbit"
NONE	"apple"	"orange"	"bananalion"	"lycheelion"	"lemon"	"apricotlion"

COLUMN KEY

number	name	state	weight	height	age	phone
NONE	"apple"	"orange"	"banana"+ ROW KEY	"lychee"+ ROW KEY	"lemon"	"apricot"+ ROW KEY

ROW KEY

number	
1	"tiger"
2	"dog"
3	"cat"
4	"mouse"
5	"elephant"
6	"cow"
7	"pig"
8	"rabbit"
9	"lion"

FIG.8

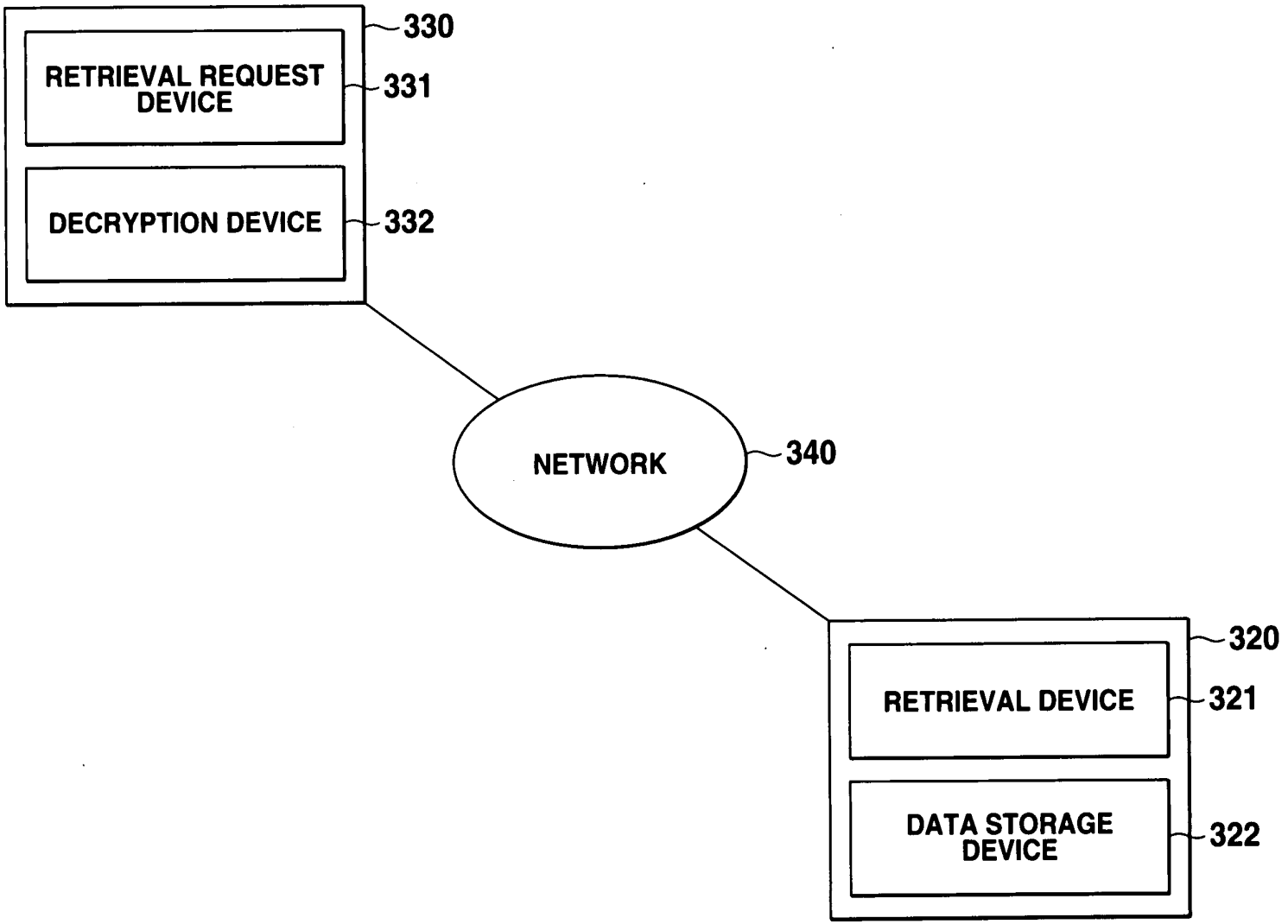
330
RETRIEVAL REQUEST DEVICE
331
DECRYPTION DEVICE
332
NETWORK
340
320
RETRIEVAL DEVICE
321
DATA STORAGE DEVICE
322

FIG.9

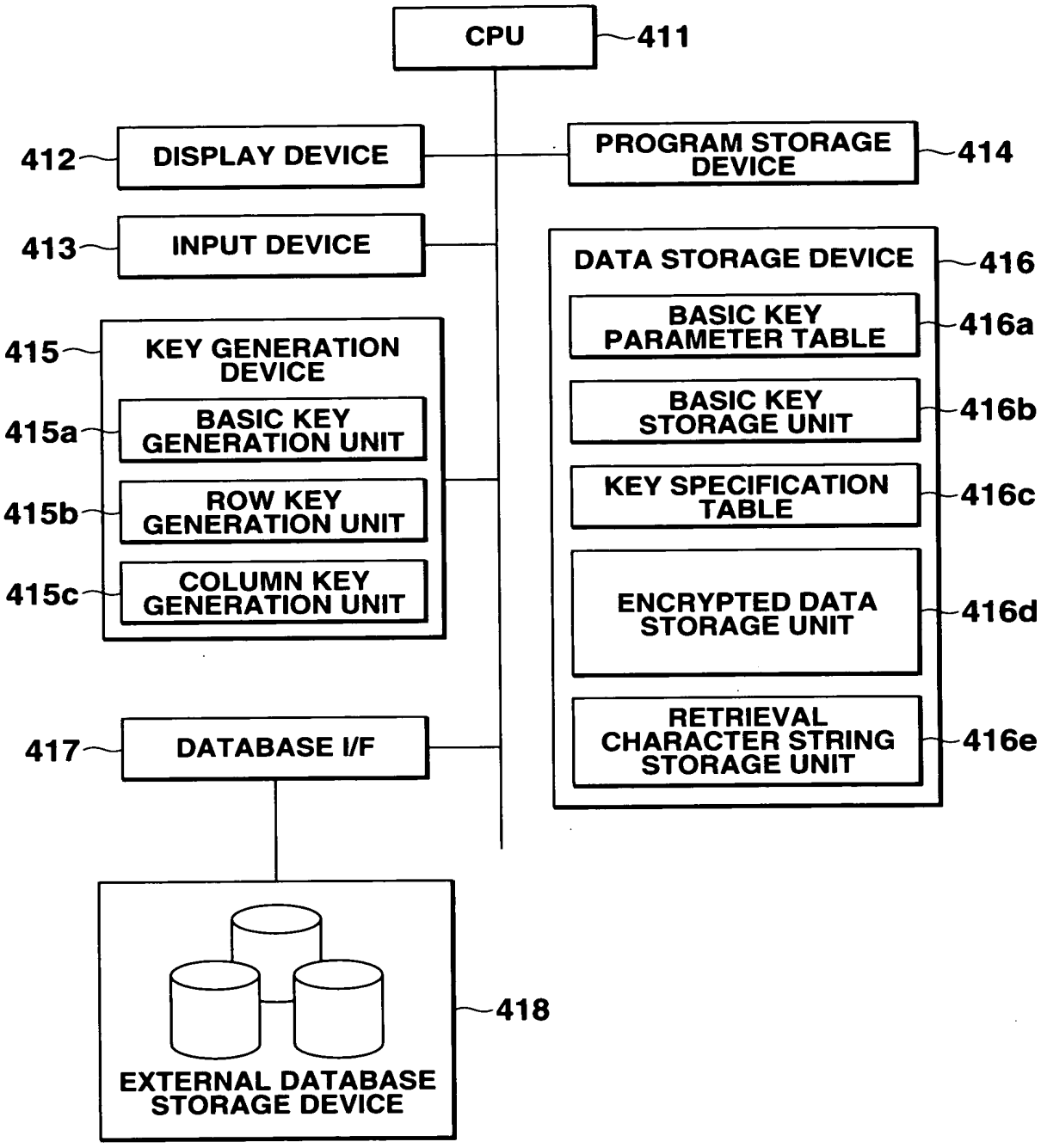
CPU
411
412
DISPLAY DEVICE
PROGRAM STORAGE DEVICE
414
413
INPUT DEVICE
DATA STORAGE DEVICE
416
BASIC KEY PARAMETER TABLE
416a
415
KEY GENERATION DEVICE
BASIC KEY STORAGE UNIT
416b
415a
BASIC KEY GENERATION UNIT
KEY SPECIFICATION TABLE
416c
415b
ROW KEY GENERATION UNIT
ENCRYPTED DATA STORAGE UNIT
416d
415c
COLUMN KEY GENERATION UNIT
RETRIEVAL CHARACTER STRING STORAGE UNIT
416e
417
DATABASE I/F
418
EXTERNAL DATABASE STORAGE DEVICE

FIG.10

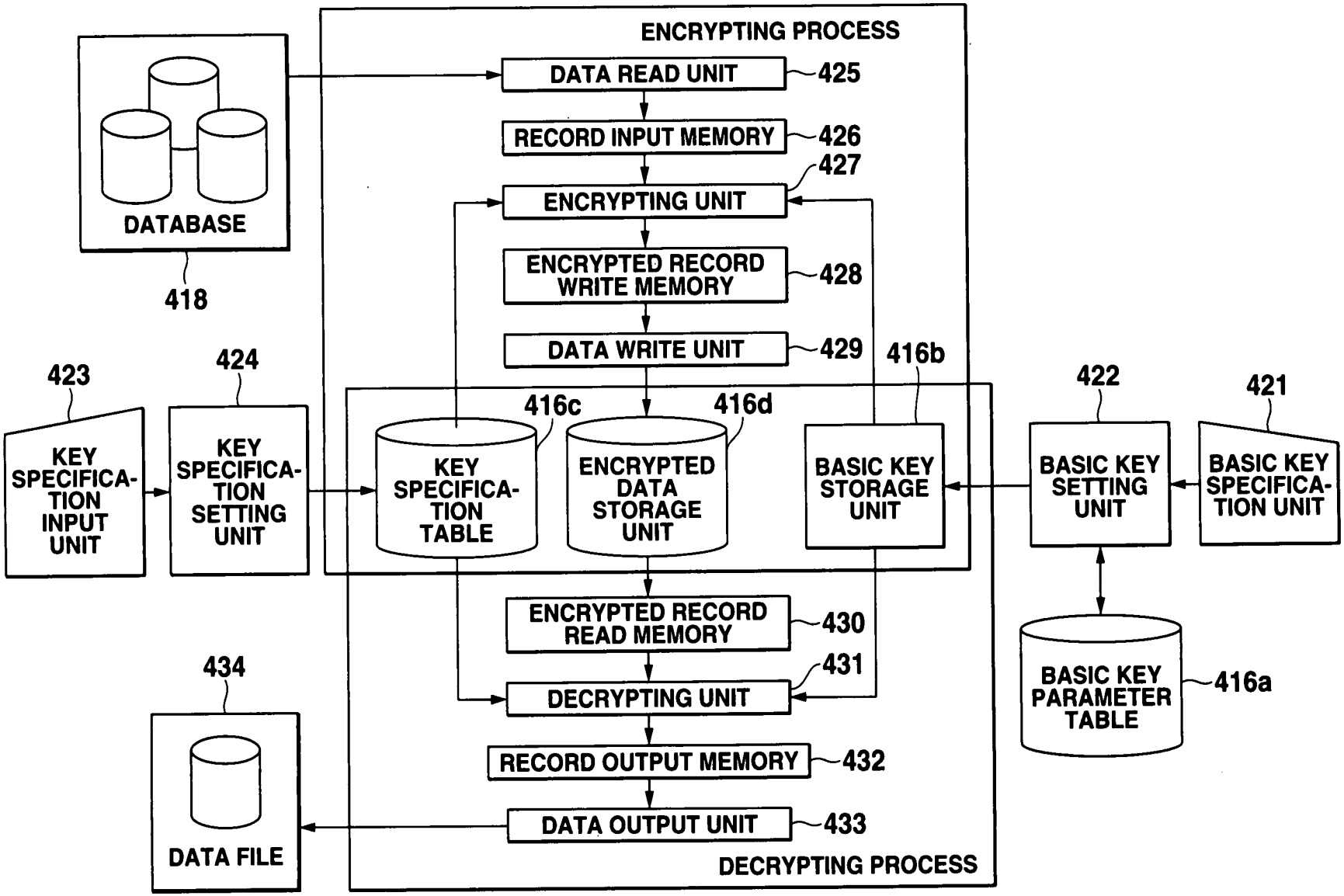
ENCRYPTING PROCESS
DATA READ UNIT
425
RECORD INPUT MEMORY
426
427
ENCRYPTING UNIT
ENCRYPTED RECORD WRITE MEMORY
428
DATA WRITE UNIT
429
DATABASE
418
423
424
416b
422
421
416c
416d
KEY SPECIFICA-TION INPUT UNIT
KEY SPECIFICA-TION SETTING UNIT
KEY SPECIFICA-TION TABLE
ENCRYPTED DATA STORAGE UNIT
BASIC KEY STORAGE UNIT
BASIC KEY SETTING UNIT
BASIC KEY SPECIFICA-TION UNIT
ENCRYPTED RECORD READ MEMORY
430
431
DECRYPTING UNIT
BASIC KEY PARAMETER TABLE
416a
434
RECORD OUTPUT MEMORY
432
DATA OUTPUT UNIT
433
DATA FILE
DECRYPTING PROCESS

FIG.11

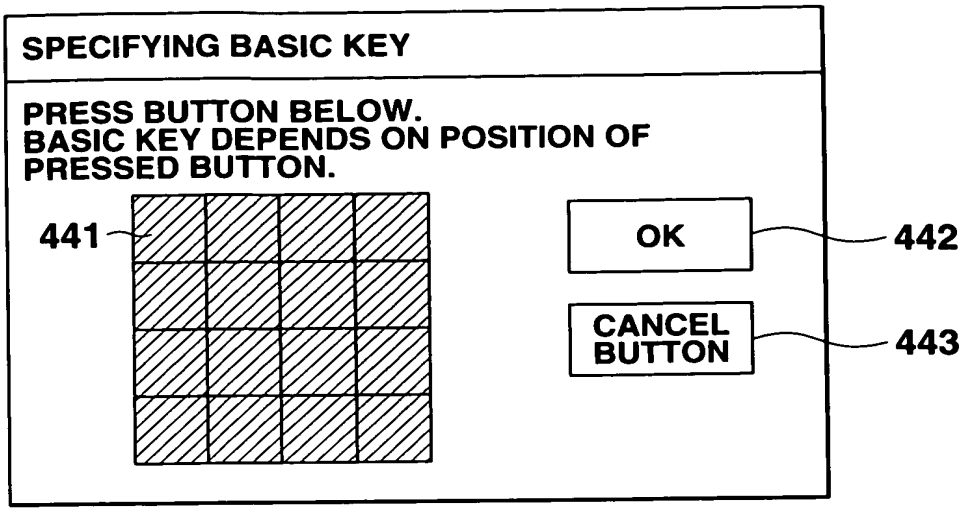

FIG.12

BASIC KEY PARAMETER TABLE

POSITION OF BUTTON	BASIC PARAMETER VALUE
1	5
2	7
3	9
4	11
5	13
6	15
7	17
8	19
9	21
10	23
11	25
12	27
13	29
14	31
15	33
16	35

416a

FIG.13

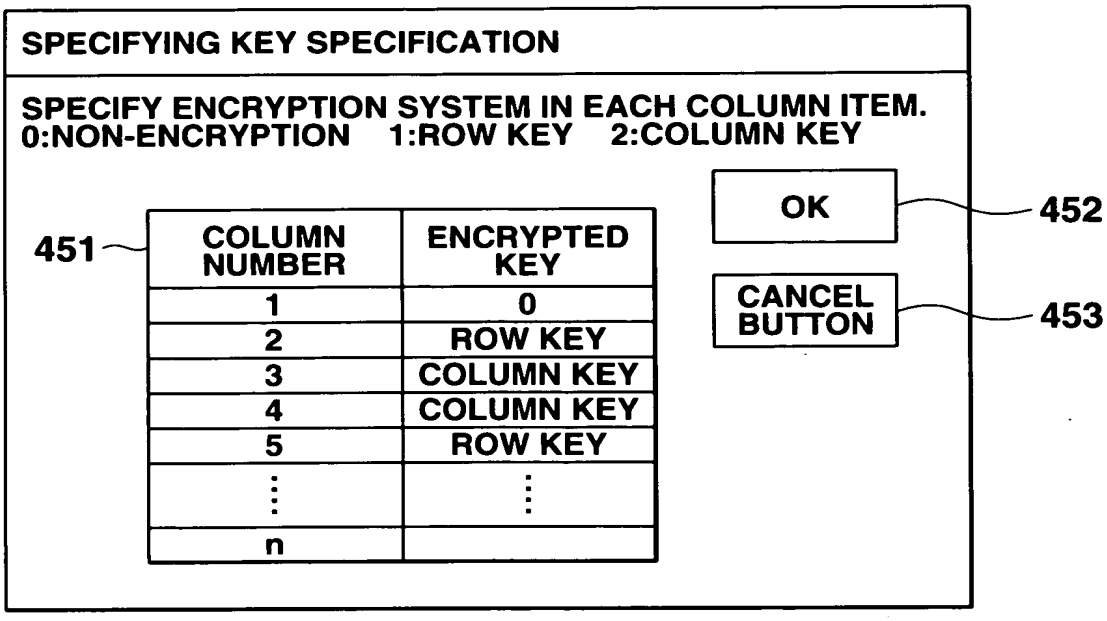

FIG.14

KEY SPECIFICATION TABLE

COLUMN NAME	COLUMN NUMBER	ENCRYPTED KEY
(code)	1	0
(name)	2	ROW KEY
(state)	3	COLUMN KEY
(age)	4	COLUMN KEY
(phone)	5	ROW KEY

416c

FIG.15

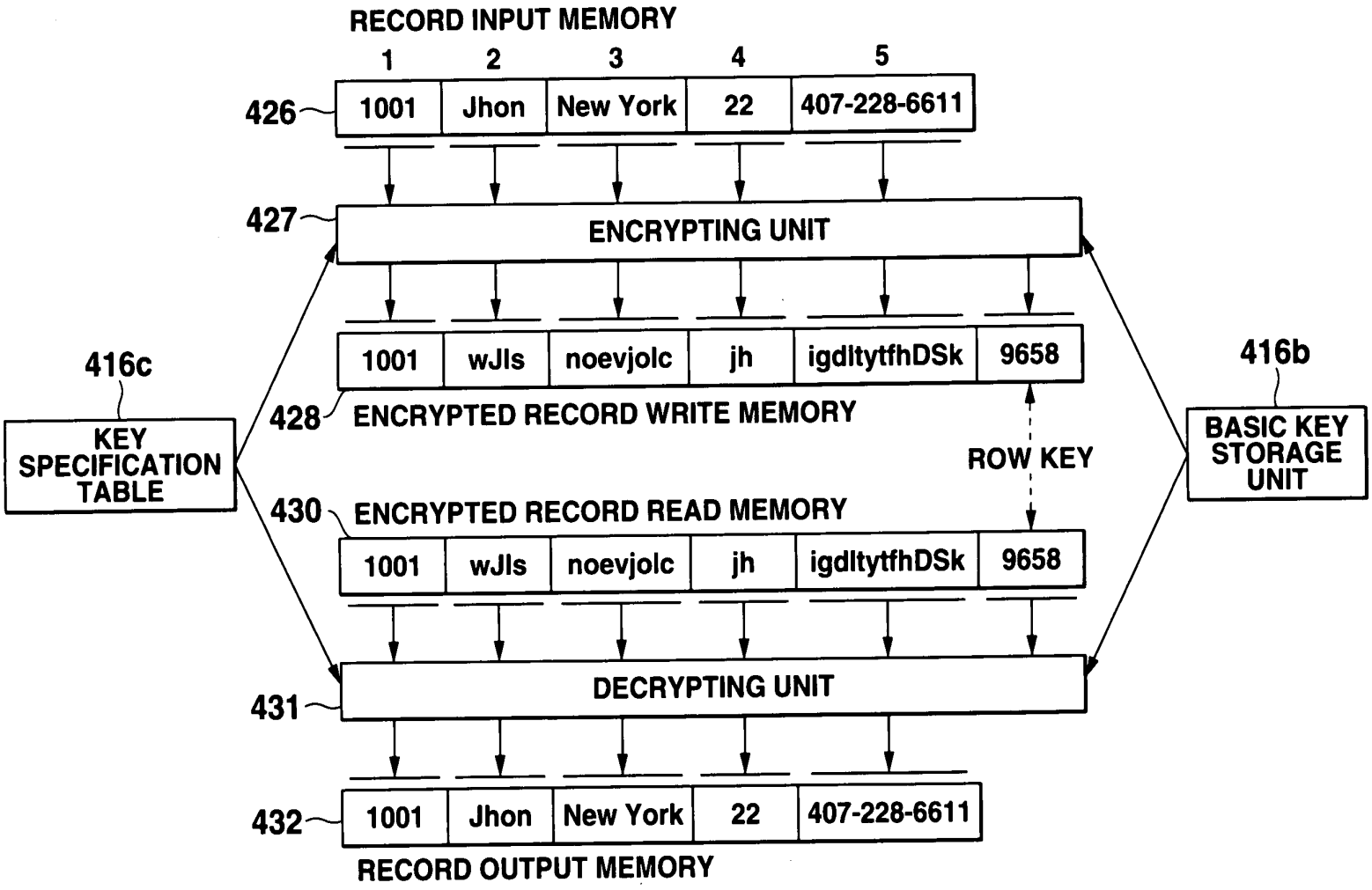
RECORD INPUT MEMORY
1
2
3
4
5
426
1001
Jhon
New York
22
407-228-6611
427
ENCRYPTING UNIT
1001
wJls
noevjolc
jh
igdltytfhDSk
9658
416c
KEY SPECIFICATION TABLE
428
ENCRYPTED RECORD WRITE MEMORY
416b
BASIC KEY STORAGE UNIT
ROW KEY
430
ENCRYPTED RECORD READ MEMORY
1001
wJls
noevjolc
jh
igdltytfhDSk
9658
431
DECRYPTING UNIT
432
1001
Jhon
New York
22
407-228-6611
RECORD OUTPUT MEMORY

FIG.16

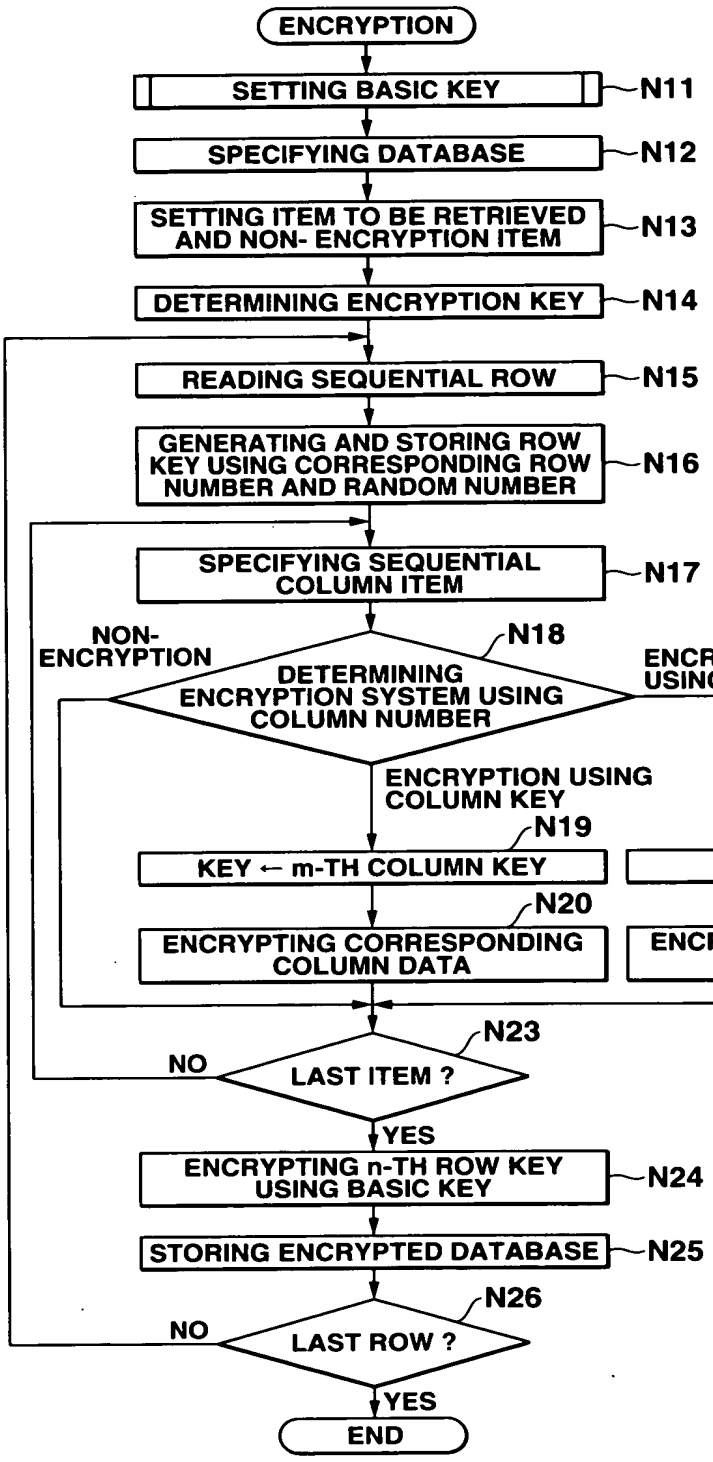

FIG.17A

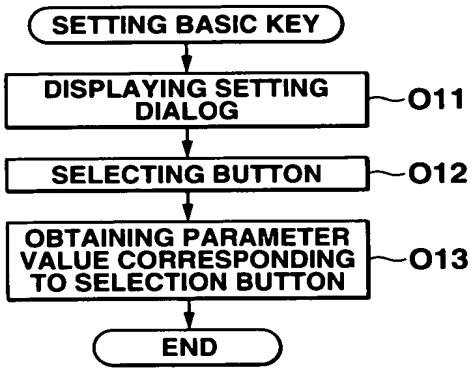

FIG.17B

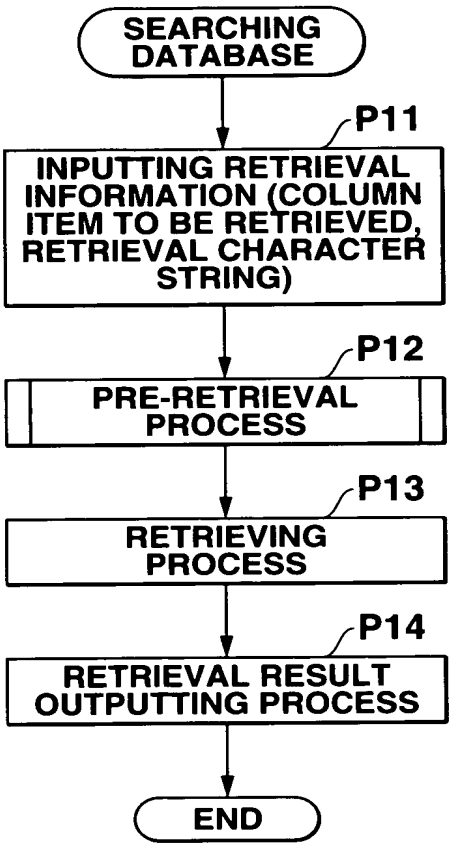

FIG.18A

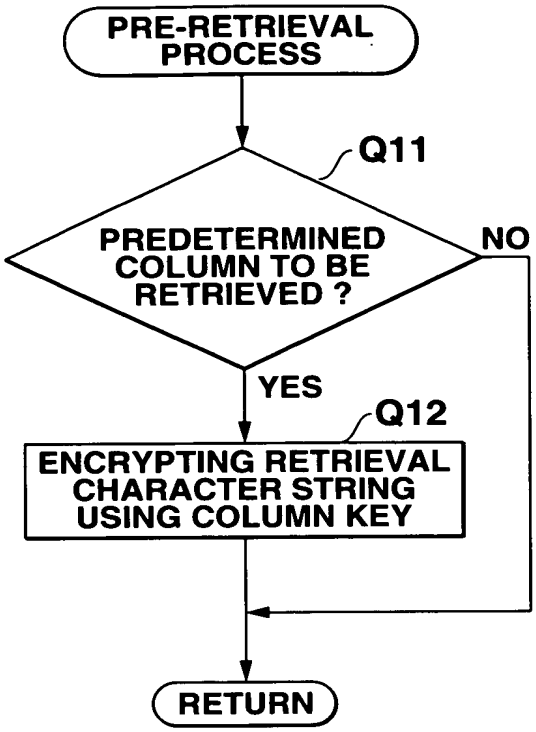

FIG.18B

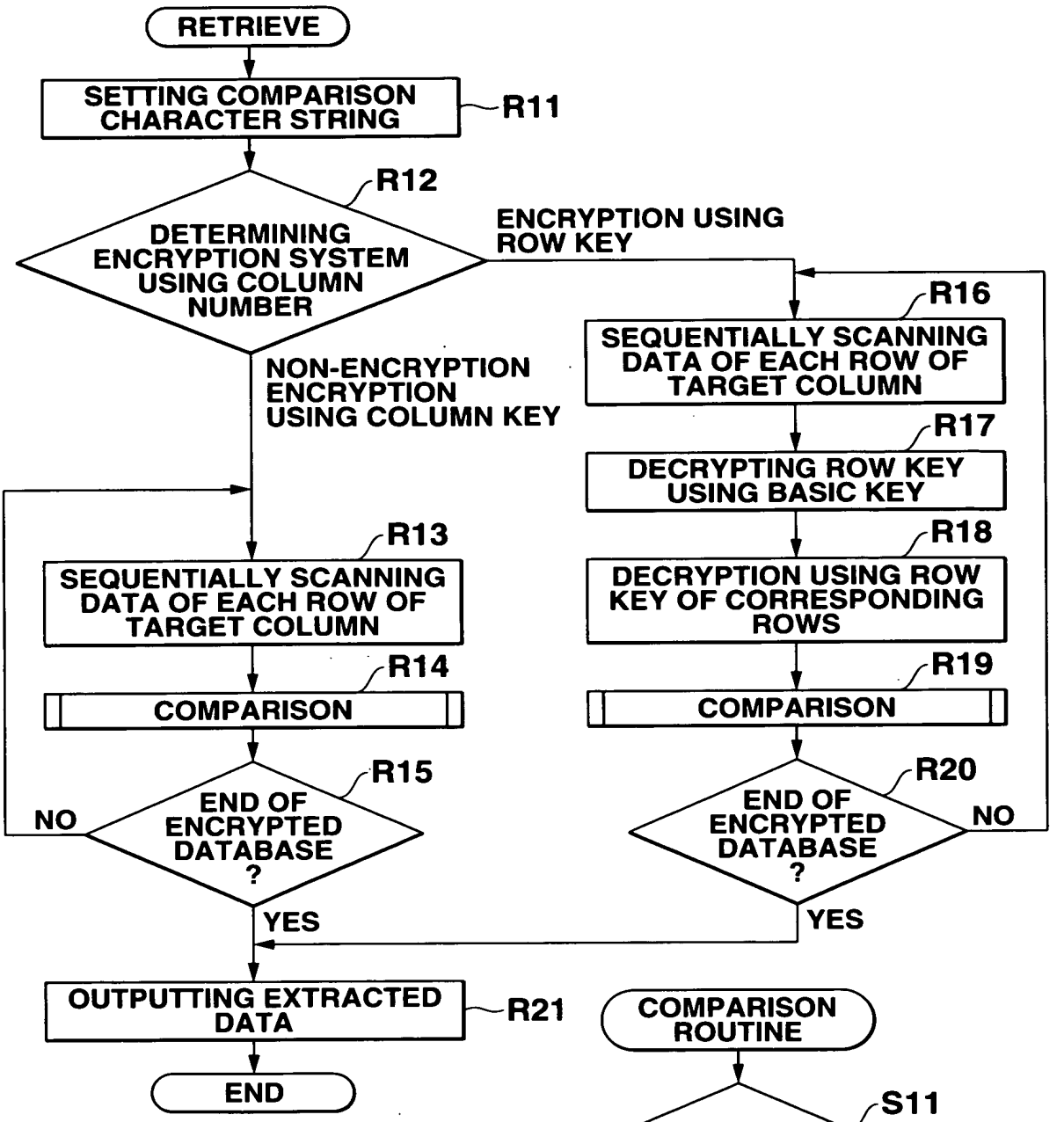

FIG.19A

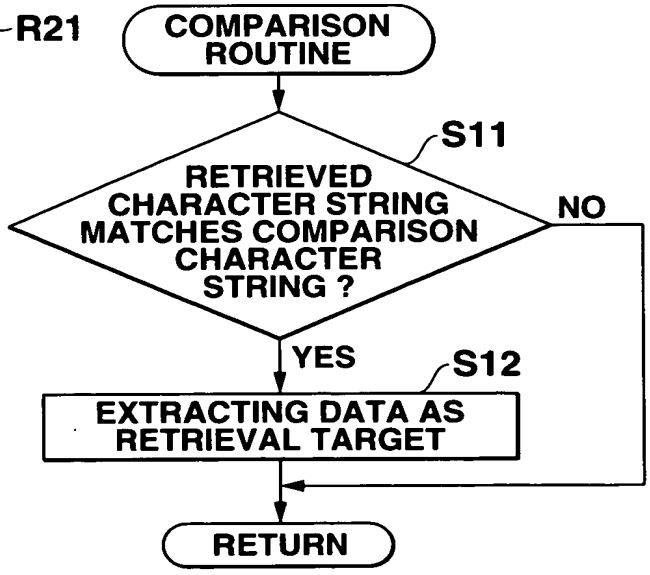

FIG.19B

(a)

number	name	state	age	phone
1001	Jhon	New York	22	407-228-6611
1002	Chris	Florida	21	123-456-7890
1003	Michael	Minnesota	27	101-202-3030
1004	David	Iowa	34	523-761-0045
1005	Mark	New York	30	832-962-9001
1006	Daniel	Iowa	25	231-981-9454
1007	George	Idaho	31	561-545-4389
1008	Henry	Florida	22	239-203-9800
1009	Joe	New Jersey	27	239-129-9898

ENCRYPTION ↓ COLUMN KEY ROW KEY

(b)

number	name	state	age	phone	line key
1001	wJls	noevjolc	jh	igdltytfhDSk	9658
1002	ddGGa	h*/fDD	hg	LKtYtDSkoKow	9143
1003	1jkjl+P	gah{6xpVd	tY	hkliiydageQk	8278
1004	3eK@s	kHHS	Kl	d+fDlKnBerJf	4358
1005	erlN	noevjolc	Gv	wsdERfvW2Sdf	5784
1006	f>sSlu	kHHS	ij	1xcVlmFmkjpo	9743
1007	(:ld?k	IJHFD	LK	kjwDkJGvfDoa	3935
1008	rhJKd	h*/fDD	jh	e419h-ka+qwH	7412
1009	ifd	ASoChijlO-	tY	qLFUiCVkj@kl	9593

DECRYPTION ↓ COLUMN KEY ROW KEY

(c)

number	name	state	age	phone
1001	Jhon	New York	22	407-228-6611
1002	Chris	Florida	21	123-456-7890
1003	Michael	Minnesota	27	101-202-3030
1004	David	Iowa	34	523-761-0045
1005	Mark	New York	30	832-962-9001
1006	Daniel	Iowa	25	231-981-9454
1007	George	Idaho	31	561-545-4389
1008	Henry	Florida	22	239-203-9800
1009	Joe	New Jersey	27	239-129-9898

FIG.20

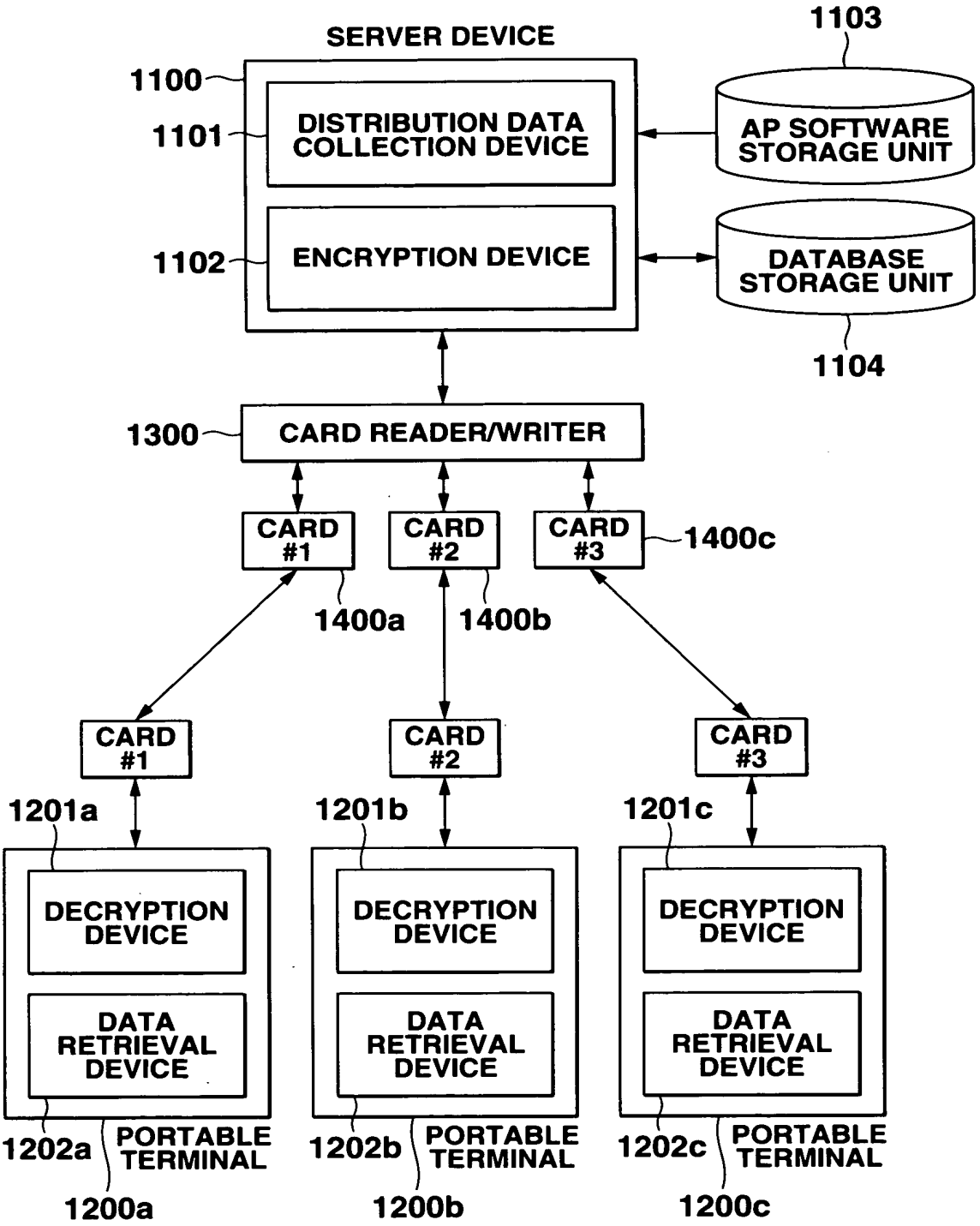
SERVER DEVICE
1100
1101
DISTRIBUTION DATA COLLECTION DEVICE
1102
ENCRYPTION DEVICE
1103
AP SOFTWARE STORAGE UNIT
DATABASE STORAGE UNIT
1104
1300
CARD READER/WRITER
CARD #1
CARD #2
CARD #3
1400c
1400a
1400b
CARD #1
CARD #2
CARD #3
1201a
1201b
1201c
DECRYPTION DEVICE
DATA RETRIEVAL DEVICE
1202a
PORTABLE TERMINAL
1200a
1202b
PORTABLE TERMINAL
1200b
1202c
PORTABLE TERMINAL
1200c

FIG.21

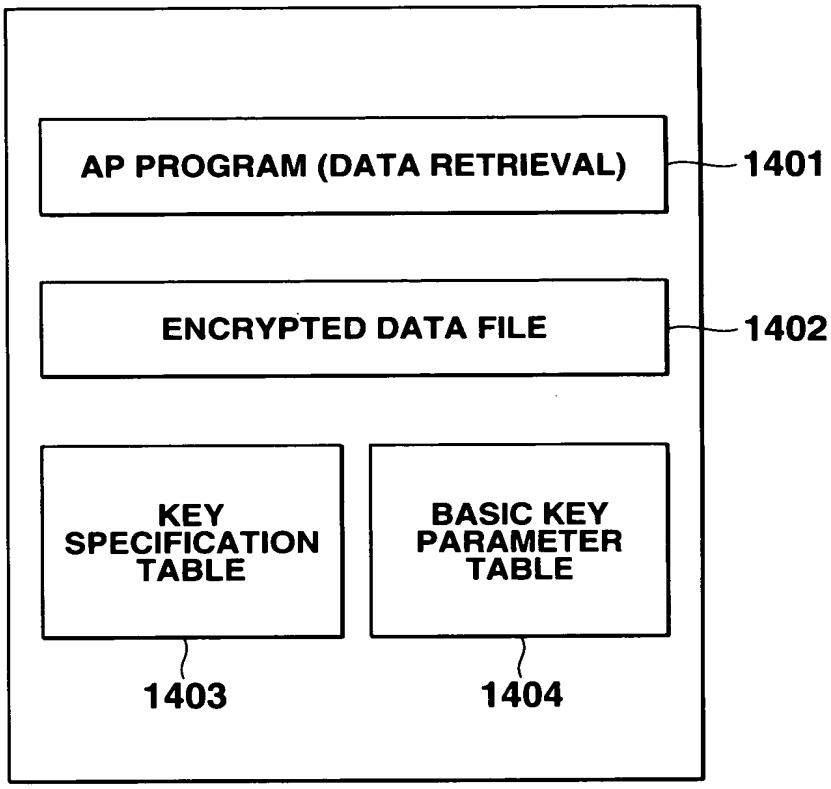
AP PROGRAM (DATA RETRIEVAL)
1401
ENCRYPTED DATA FILE
1402
KEY SPECIFICATION TABLE
BASIC KEY PARAMETER TABLE
1403
1404

FIG.22

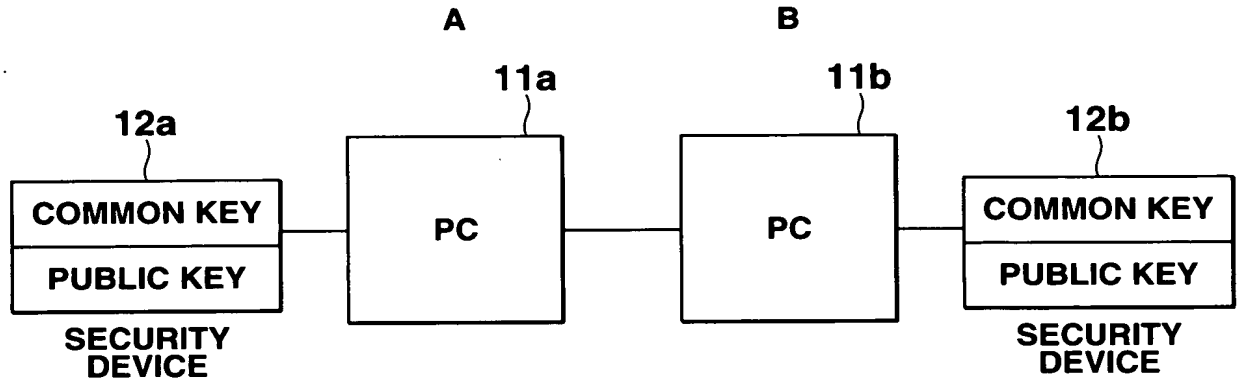
A
B
11a
11b
12a
12b
COMMON KEY
PUBLIC KEY
SECURITY DEVICE
PC
PC
COMMON KEY
PUBLIC KEY
SECURITY DEVICE

FIG.23

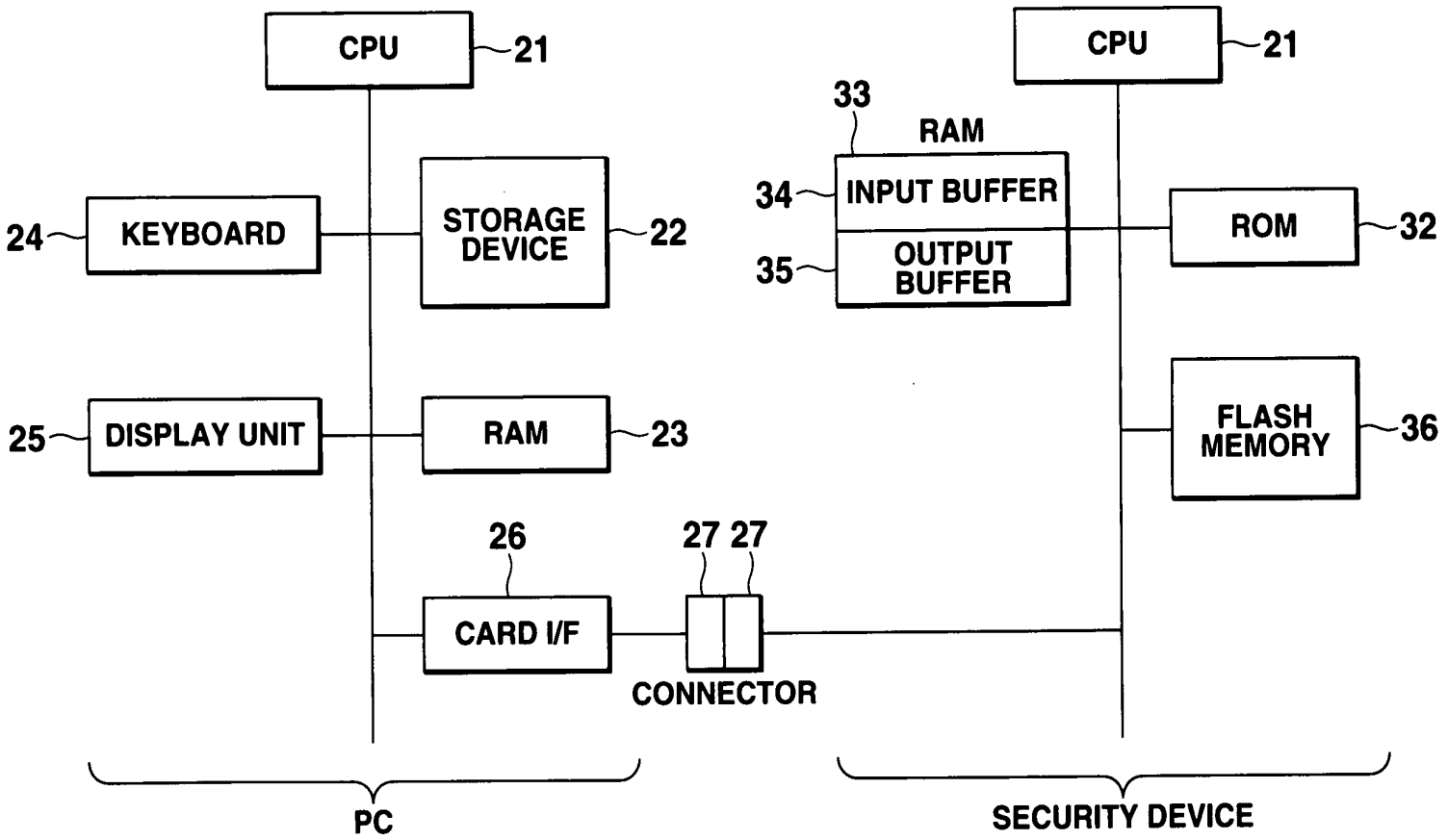
CPU
21
24
KEYBOARD
STORAGE DEVICE
22
25
DISPLAY UNIT
RAM
23
26
CARD I/F
27 27
CONNECTOR
PC
CPU
21
33
RAM
34
INPUT BUFFER
35
OUTPUT BUFFER
ROM
32
FLASH MEMORY
36
SECURITY DEVICE

FIG.24

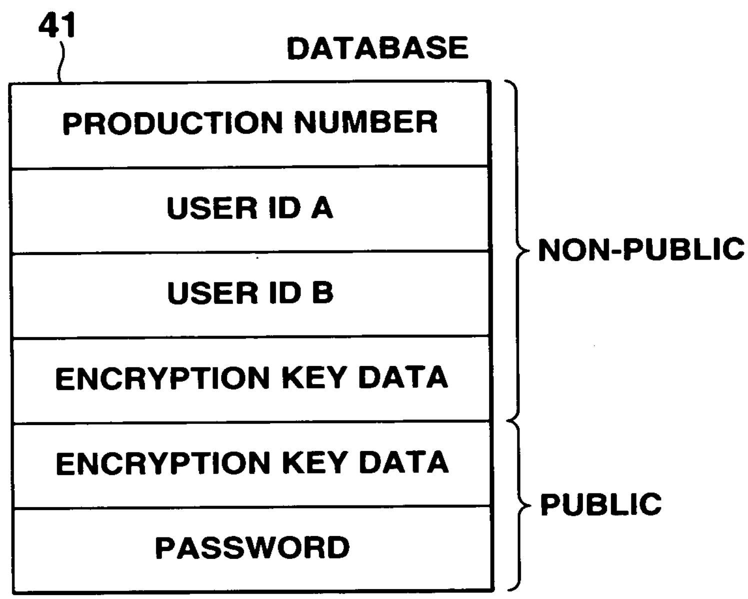
41
DATABASE
PRODUCTION NUMBER
USER ID A
USER ID B
ENCRYPTION KEY DATA
ENCRYPTION KEY DATA
PASSWORD
NON-PUBLIC
PUBLIC

FIG.25

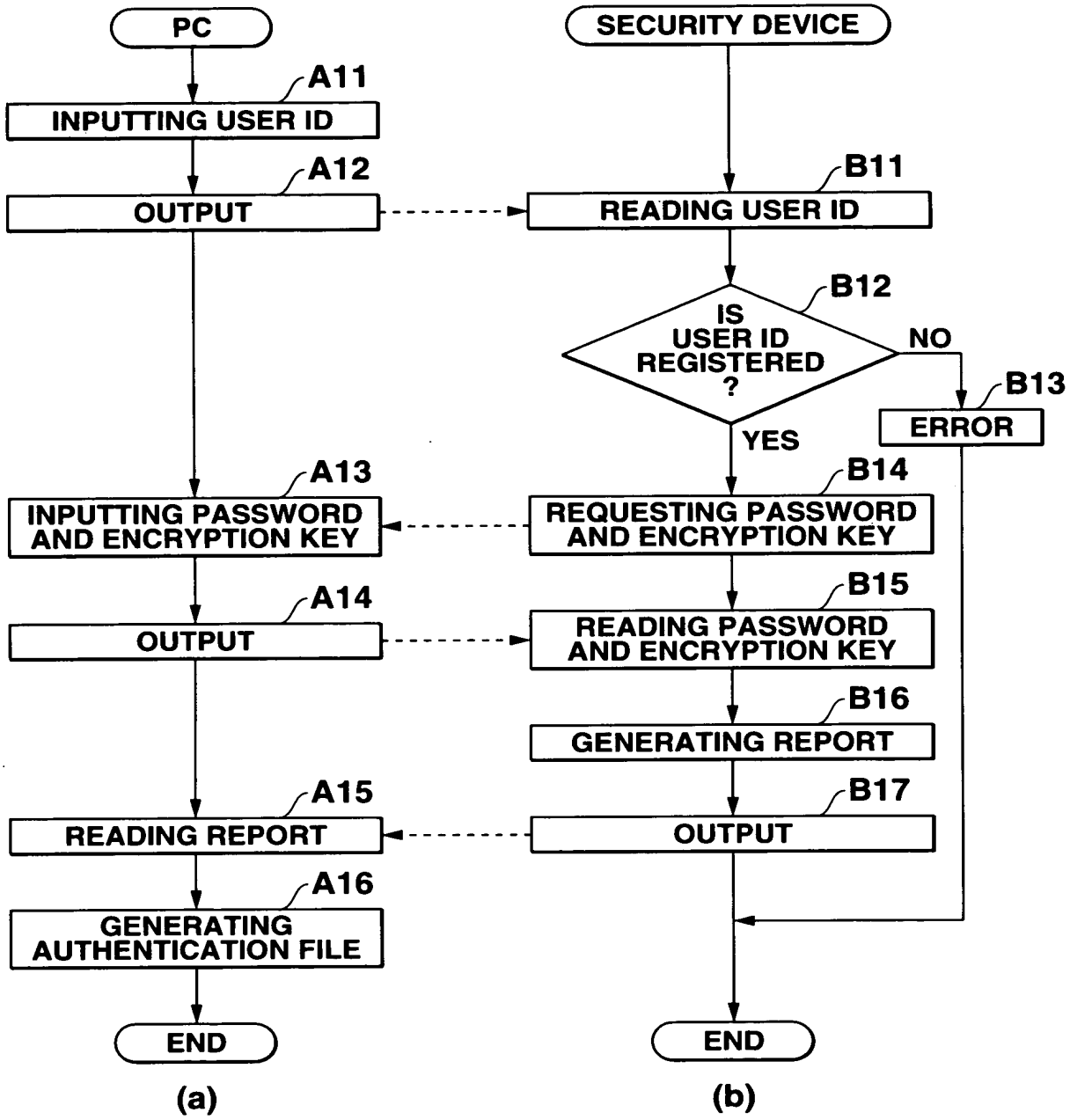
PC
A11
INPUTTING USER ID
A12
OUTPUT
A13
INPUTTING PASSWORD AND ENCRYPTION KEY
A14
OUTPUT
A15
READING REPORT
A16
GENERATING AUTHENTICATION FILE
END
(a)
SECURITY DEVICE
B11
READING USER ID
B12
IS USER ID REGISTERED ?
NO
B13
ERROR
YES
B14
REQUESTING PASSWORD AND ENCRYPTION KEY
B15
READING PASSWORD AND ENCRYPTION KEY
B16
GENERATING REPORT
B17
OUTPUT
END
(b)

FIG.26

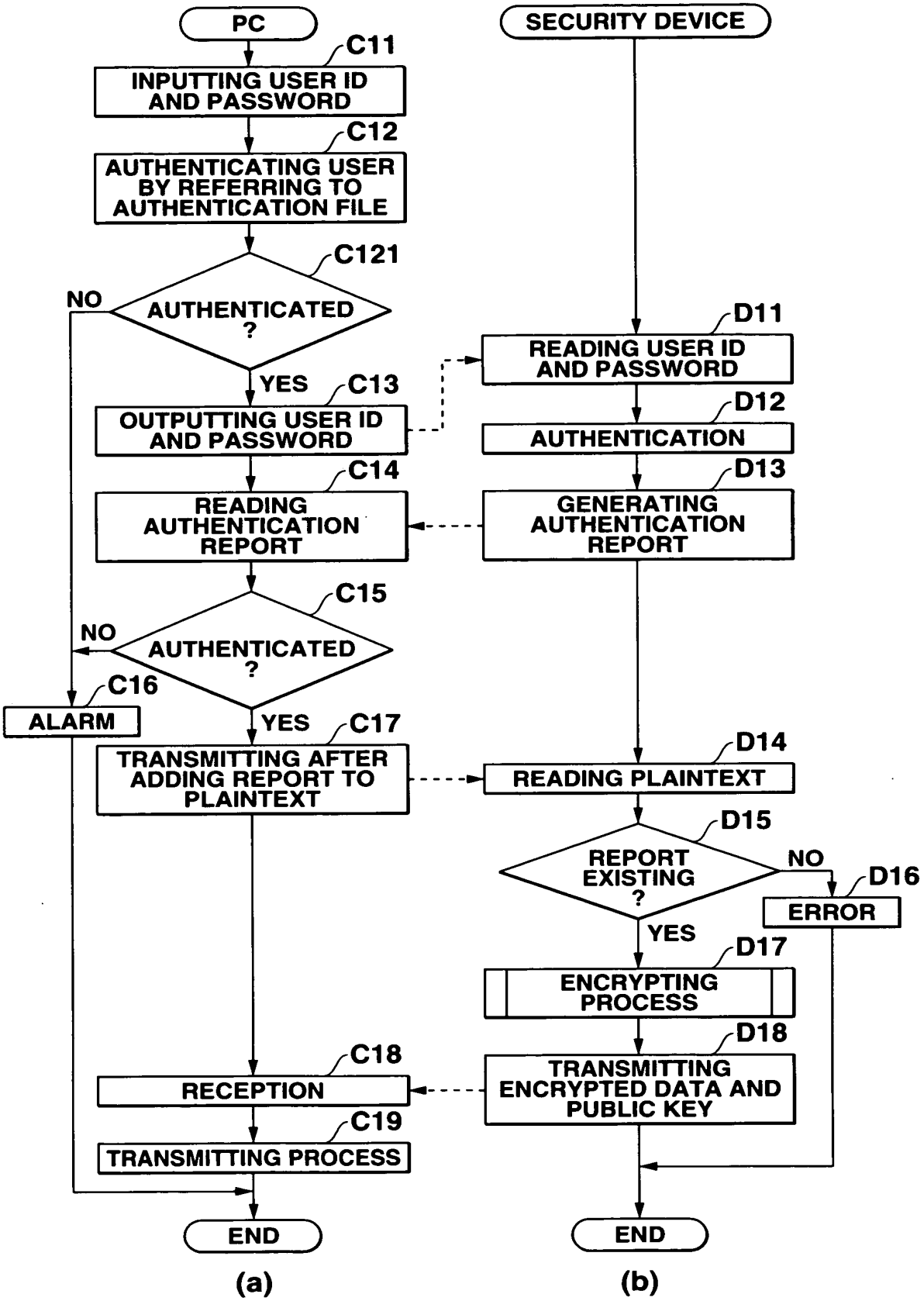
PC
C11
INPUTTING USER ID AND PASSWORD
C12
AUTHENTICATING USER BY REFERRING TO AUTHENTICATION FILE
C121
AUTHENTICATED ?
NO
YES
C13
OUTPUTTING USER ID AND PASSWORD
C14
READING AUTHENTICATION REPORT
C15
AUTHENTICATED ?
NO
C16
ALARM
YES
C17
TRANSMITTING AFTER ADDING REPORT TO PLAINTEXT
C18
RECEPTION
C19
TRANSMITTING PROCESS
END
(a)
SECURITY DEVICE
D11
READING USER ID AND PASSWORD
D12
AUTHENTICATION
D13
GENERATING AUTHENTICATION REPORT
D14
READING PLAINTEXT
D15
REPORT EXISTING ?
NO
D16
ERROR
YES
D17
ENCRYPTING PROCESS
D18
TRANSMITTING ENCRYPTED DATA AND PUBLIC KEY
END
(b)

FIG.27

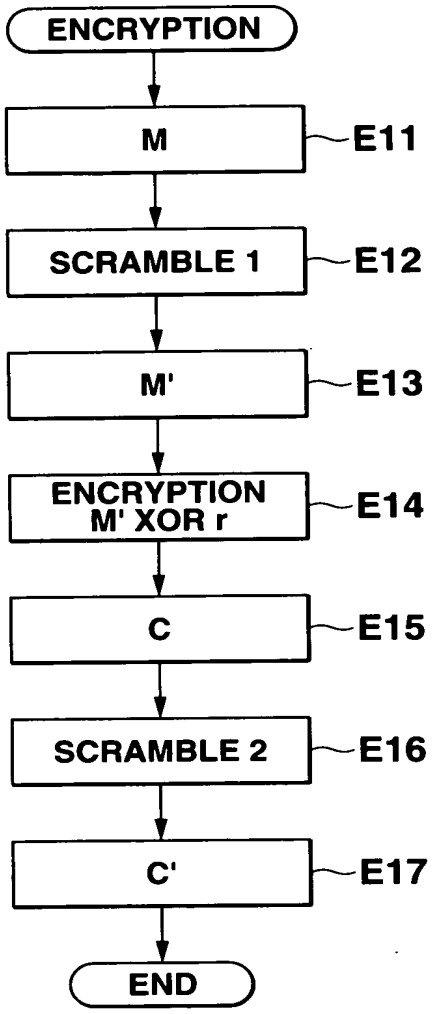

FIG.28A

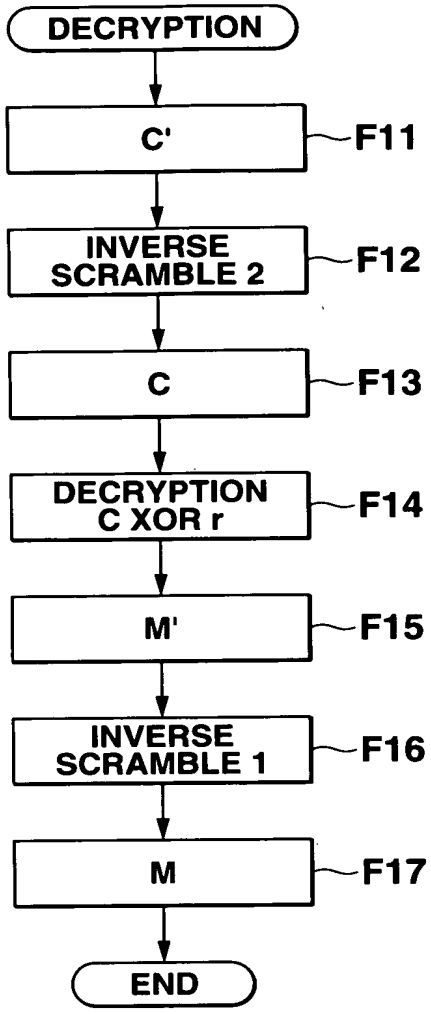

FIG.28B

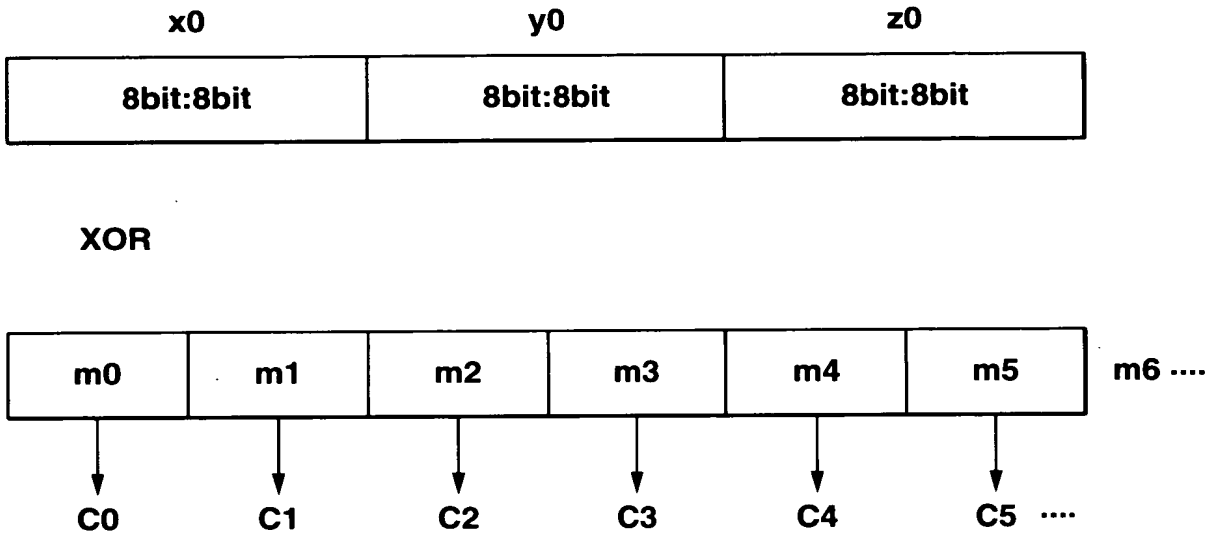
x0
y0
z0
8bit:8bit
8bit:8bit
8bit:8bit
XOR
m0
m1
m2
m3
m4
m5
m6 ····
C0
C1
C2
C3
C4
C5 ····

FIG.29

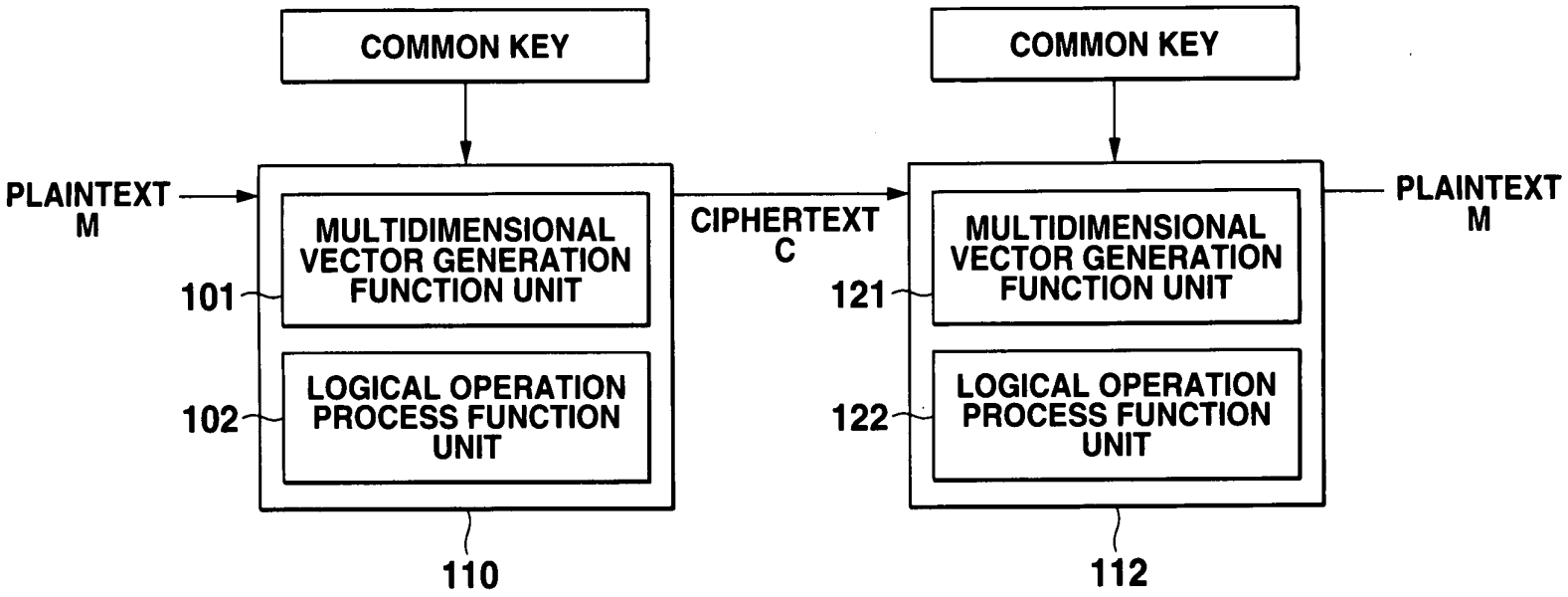
COMMON KEY
COMMON KEY
PLAINTEXT
M
MULTIDIMENSIONAL VECTOR GENERATION FUNCTION UNIT
101
LOGICAL OPERATION PROCESS FUNCTION UNIT
102
110
CIPHERTEXT
C
MULTIDIMENSIONAL VECTOR GENERATION FUNCTION UNIT
121
LOGICAL OPERATION PROCESS FUNCTION UNIT
122
112
PLAINTEXT
M

FIG.30

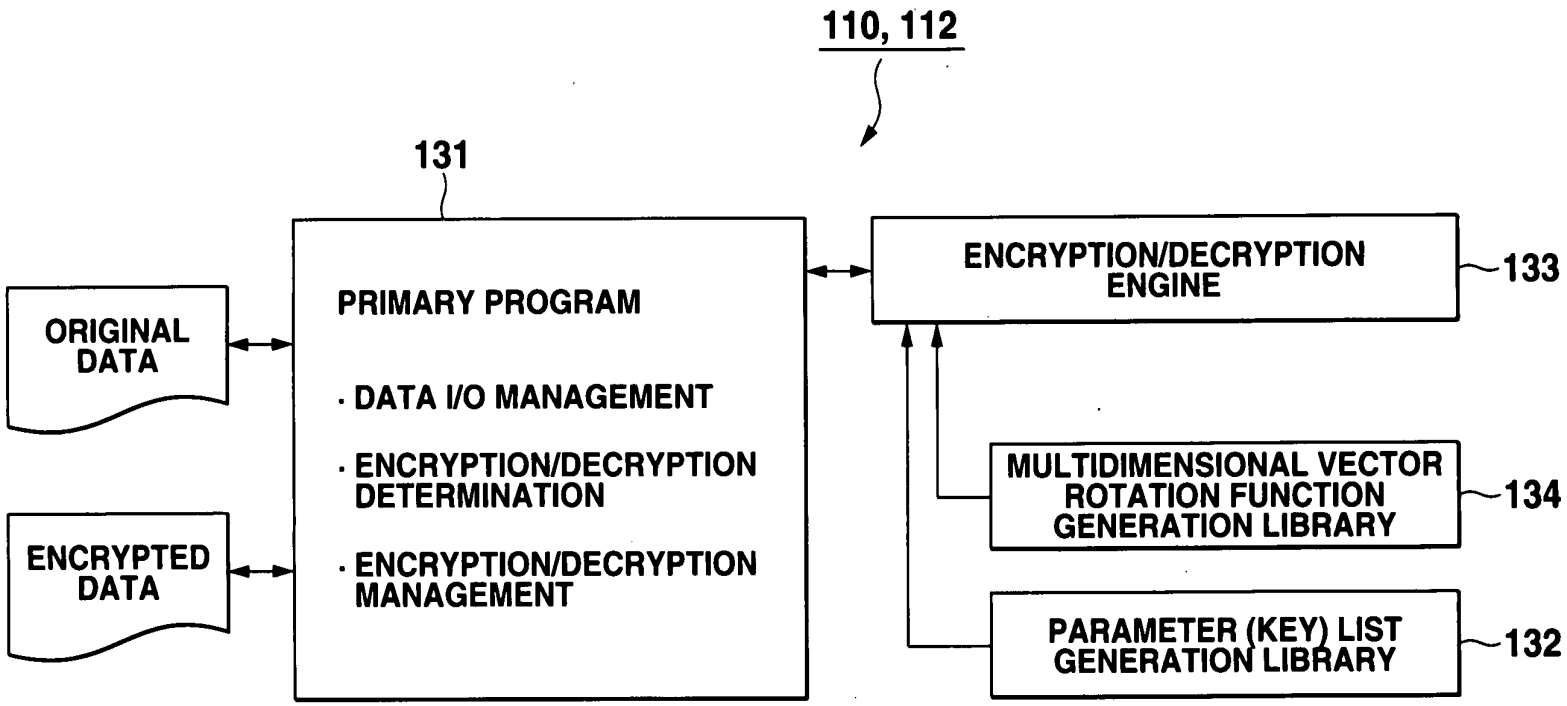
110, 112
131
PRIMARY PROGRAM
· DATA I/O MANAGEMENT
· ENCRYPTION/DECRYPTION DETERMINATION
· ENCRYPTION/DECRYPTION MANAGEMENT
ORIGINAL DATA
ENCRYPTED DATA
ENCRYPTION/DECRYPTION ENGINE
133
MULTIDIMENSIONAL VECTOR ROTATION FUNCTION GENERATION LIBRARY
134
PARAMETER (KEY) LIST GENERATION LIBRARY
132

FIG.31

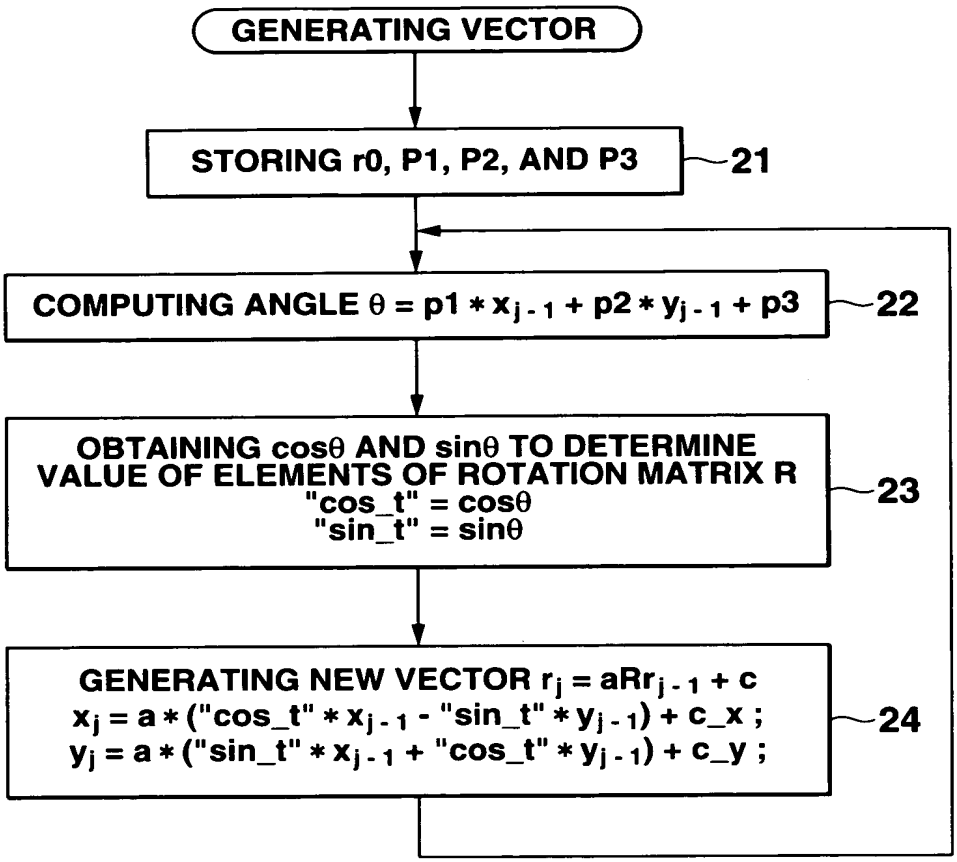
GENERATING VECTOR
STORING r0, P1, P2, AND P3
21
COMPUTING ANGLE θ = p1 * x j - 1 + p2 * y j - 1 + p3
22
OBTAINING cosθ AND sinθ TO DETERMINE VALUE OF ELEMENTS OF ROTATION MATRIX R
"cos_t" = cosθ
"sin_t" = sinθ
23
GENERATING NEW VECTOR r j = aRr j - 1 + c
x j = a * ("cos_t" * x j - 1 - "sin_t" * y j - 1) + c_x ;
y j = a * ("sin_t" * x j - 1 + "cos_t" * y j - 1) + c_y ;
24

FIG.32

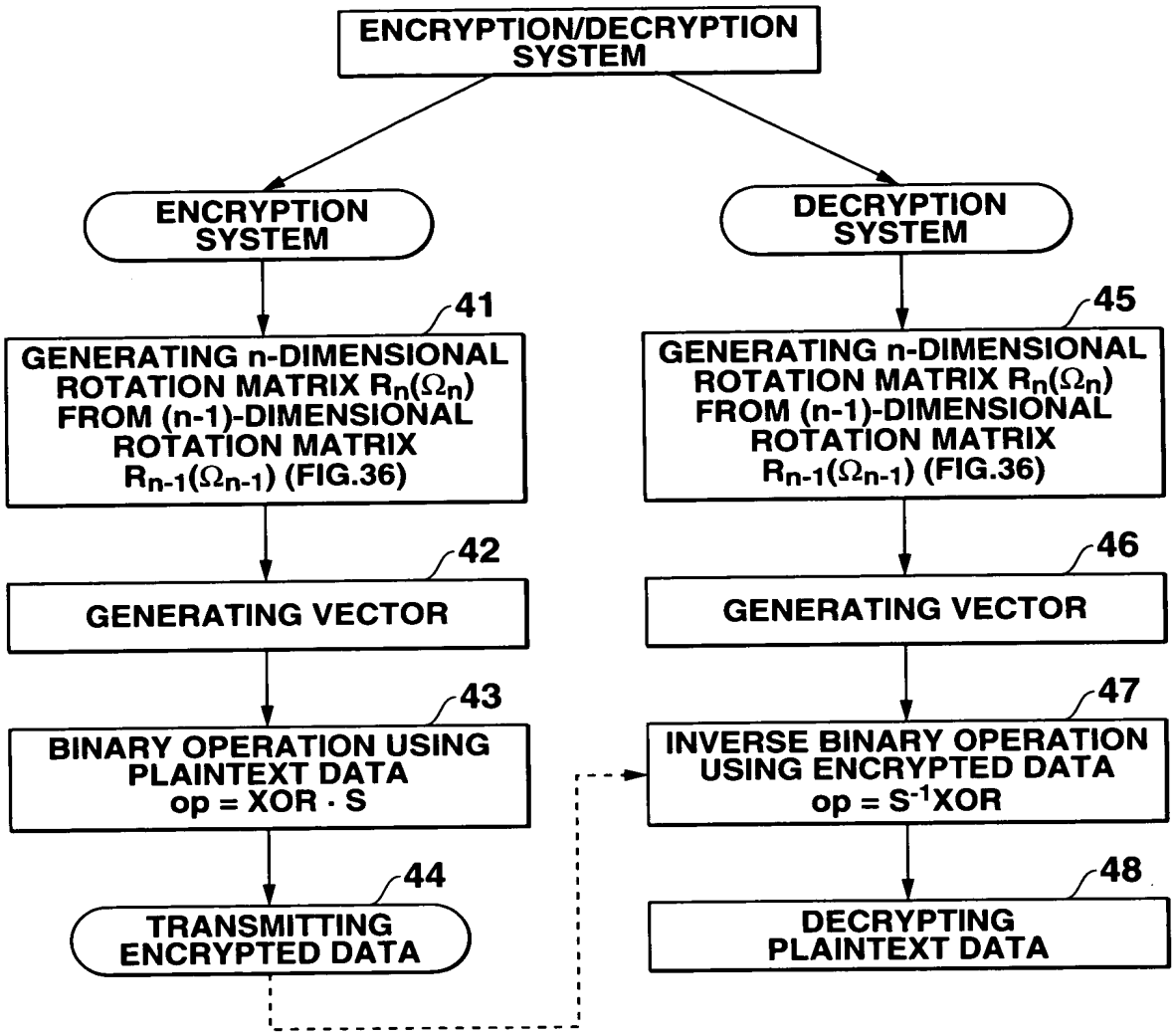
ENCRYPTION/DECRYPTION SYSTEM
ENCRYPTION SYSTEM
DECRYPTION SYSTEM
41
GENERATING n-DIMENSIONAL ROTATION MATRIX $R_n(\Omega_n)$ FROM (n-1)-DIMENSIONAL ROTATION MATRIX $R_{n-1}(\Omega_{n-1})$ (FIG.36)
42
GENERATING VECTOR
43
BINARY OPERATION USING PLAINTEXT DATA op = XOR · S
44
TRANSMITTING ENCRYPTED DATA
45
GENERATING n-DIMENSIONAL ROTATION MATRIX $R_n(\Omega_n)$ FROM (n-1)-DIMENSIONAL ROTATION MATRIX $R_{n-1}(\Omega_{n-1})$ (FIG.36)
46
GENERATING VECTOR
47
INVERSE BINARY OPERATION USING ENCRYPTED DATA op = S^{-1}XOR
48
DECRYPTING PLAINTEXT DATA

FIG.33

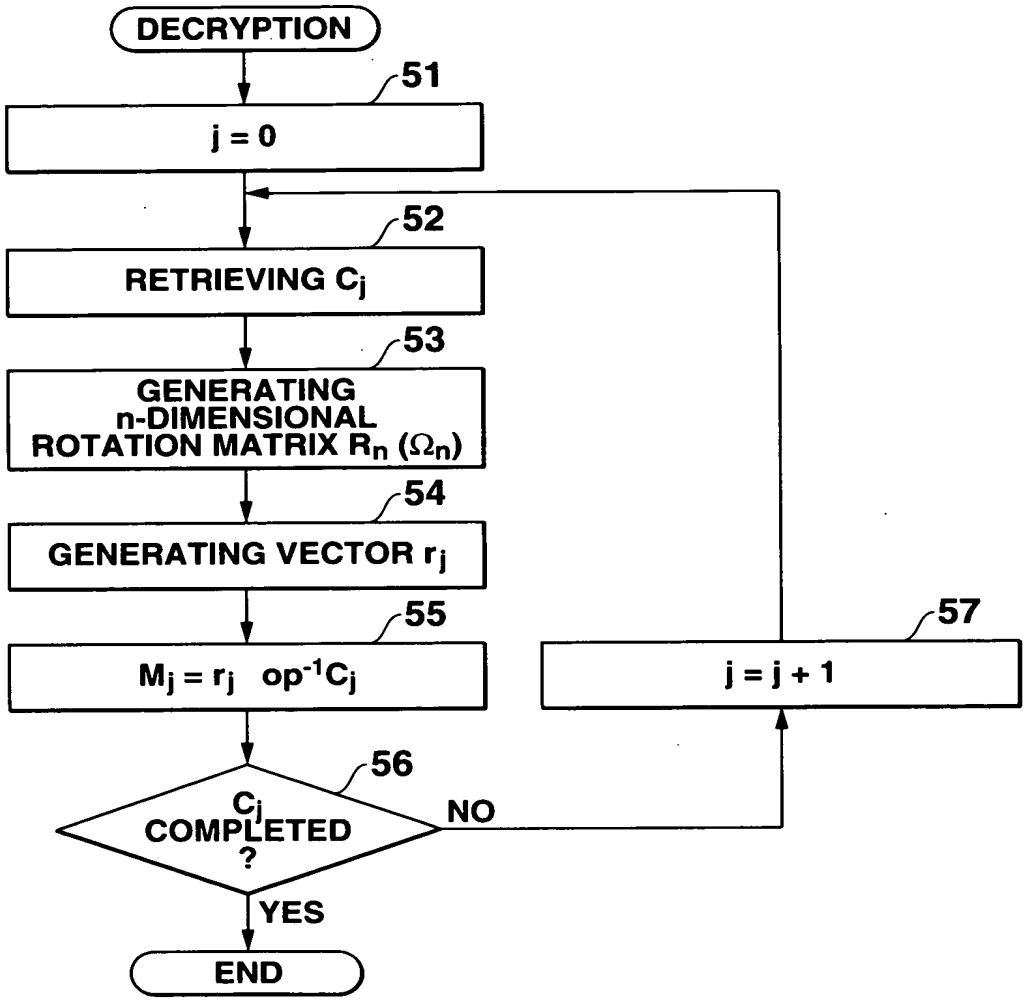
DECRYPTION
51
j = 0
52
RETRIEVING C_j
53
GENERATING n-DIMENSIONAL ROTATION MATRIX R_n (Ω_n)
54
GENERATING VECTOR r_j
55
$M_j = r_j \ op^{-1} C_j$
56
C_j COMPLETED ?
NO
YES
END
57
j = j + 1

FIG.34

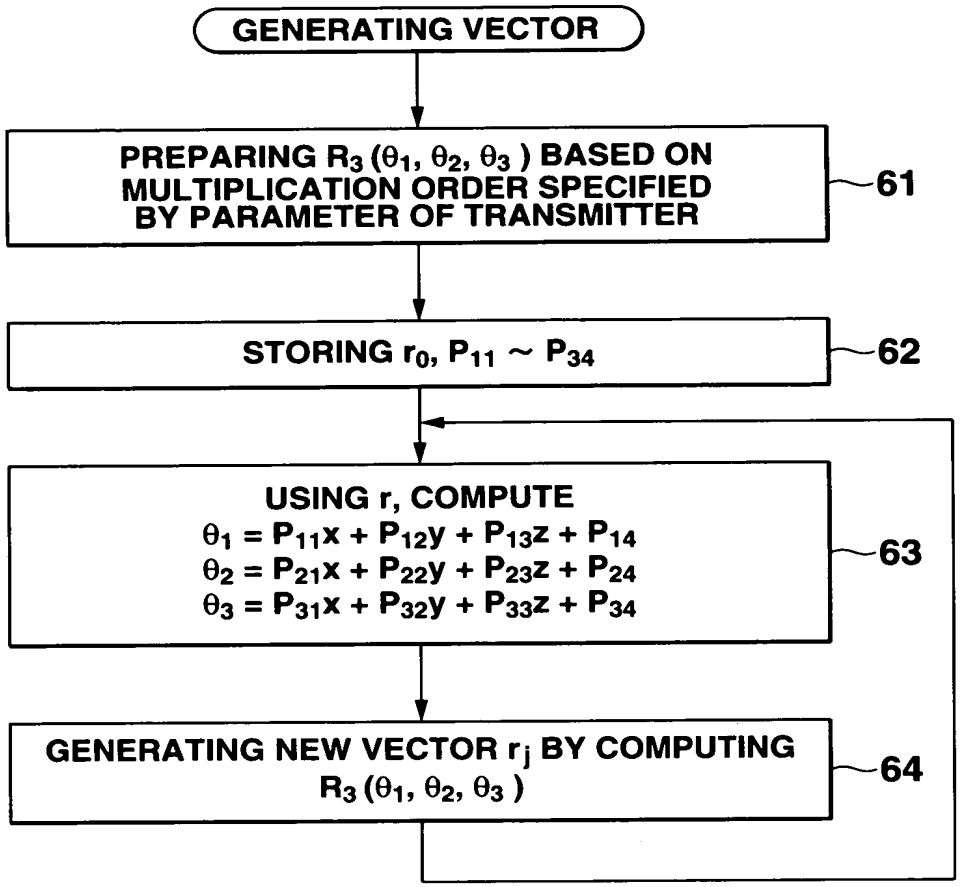
GENERATING VECTOR
PREPARING $R_3(\theta_1, \theta_2, \theta_3)$ BASED ON MULTIPLICATION ORDER SPECIFIED BY PARAMETER OF TRANSMITTER
61
STORING r_0, $P_{11} \sim P_{34}$
62
USING r, COMPUTE
$\theta_1 = P_{11}x + P_{12}y + P_{13}z + P_{14}$
$\theta_2 = P_{21}x + P_{22}y + P_{23}z + P_{24}$
$\theta_3 = P_{31}x + P_{32}y + P_{33}z + P_{34}$
63
GENERATING NEW VECTOR r_j BY COMPUTING $R_3(\theta_1, \theta_2, \theta_3)$
64

FIG.35

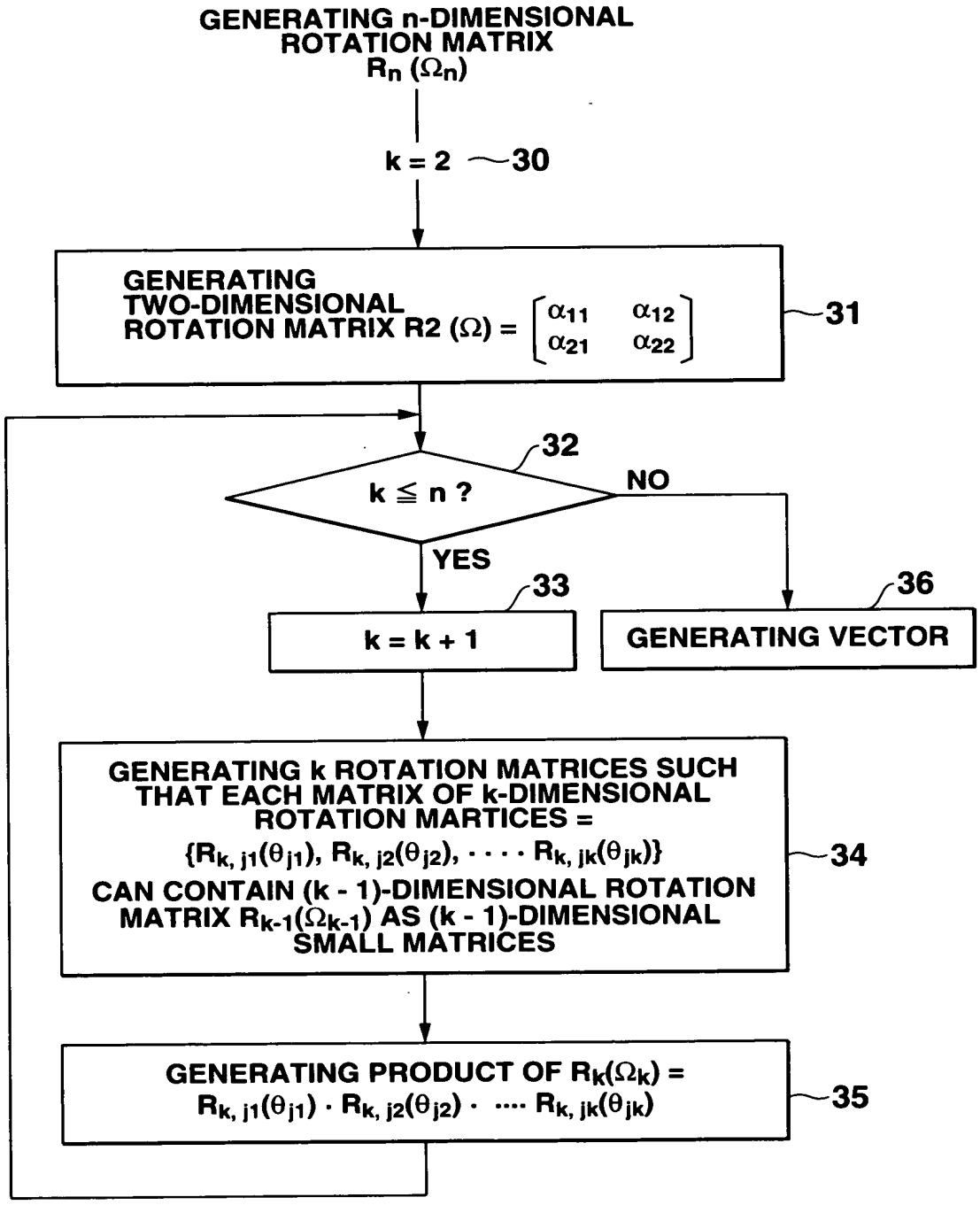
GENERATING n-DIMENSIONAL ROTATION MATRIX $R_n(\Omega_n)$
k = 2
30
GENERATING TWO-DIMENSIONAL ROTATION MATRIX R2 (Ω) = $\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$
31
32
k ≦ n ?
NO
YES
33
k = k + 1
36
GENERATING VECTOR
GENERATING k ROTATION MATRICES SUCH THAT EACH MATRIX OF k-DIMENSIONAL ROTATION MARTICES =
$\{R_{k,j1}(\theta_{j1}), R_{k,j2}(\theta_{j2}), \cdots R_{k,jk}(\theta_{jk})\}$
CAN CONTAIN (k - 1)-DIMENSIONAL ROTATION MATRIX $R_{k-1}(\Omega_{k-1})$ AS (k - 1)-DIMENSIONAL SMALL MATRICES
34
GENERATING PRODUCT OF $R_k(\Omega_k)$ =
$R_{k,j1}(\theta_{j1}) \cdot R_{k,j2}(\theta_{j2}) \cdot \cdots R_{k,jk}(\theta_{jk})$
35

FIG.36

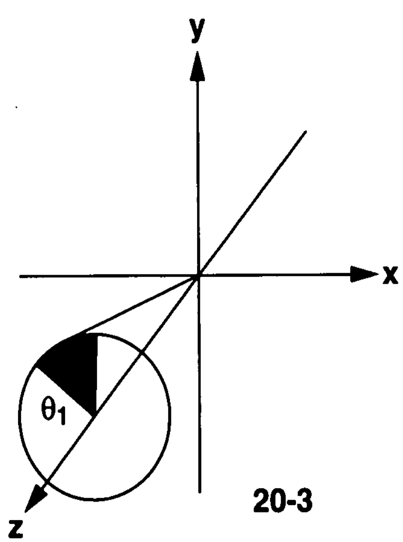

FIG.37A

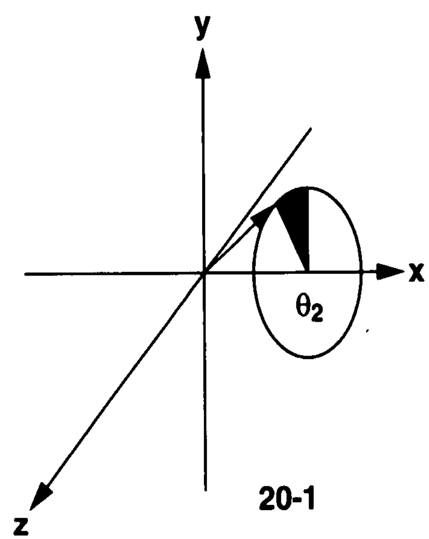

FIG.37B

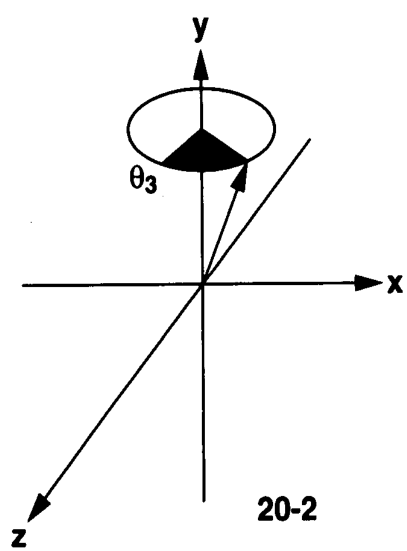

FIG.37C